AN INFORMATIONAL ANALYSIS AND COMMUNICATIONS SQUADRON SURVEY OF CYBERSPACE MISSION ASSURANCE

GRADUATE RESEARCH PROJECT

Mickey R. Evans, Major, USAF

AFIT/IDE/ENV/10-J01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY
AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/IDE/ENV/10-J01

AN INFORMATIONAL ANALYSIS AND COMMUNICATIONS SQUADRON SURVEY OF CYBERSPACE MISSION ASSURANCE

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Cyber Warfare

Mickey R. Evans, MA

Major, USAF

June 2010

AFIT/IDE/ENV/10-J01

AN INFORMATIONAL ANALYSIS AND COMMUNICATIONS SQUADRON SURVEY OF CYBERSPACE MISSION ASSURANCE

Mickey R. Evans, MA
Major, USAF

Approved:

___/signed/_____	7 June 2010
Michael R. Grimaila, PhD (Chairman)	Date
___/signed/_____	8 June 2010
Robert F. Mills, PhD (Member)	Date

Abstract

Networks under the Air Force's purview are under constant attack from hostile actors. The dependence on these systems by every facet of the Air Force enterprise is more prevalent now than ever before. The realization of these facts has increased the focus on assuring more than the network systems and applications themselves, but instead on the missions that rely so heavily on the systems.

The purpose of this research is to investigate the current state of cyber mission assurance efforts and guidance available in both the public and private sector and to establish the realities facing base level units. Specifically, this graduate research project sought to answer two research questions addressing guidance and unit realities: What, if any, regulatory guidance is available, to include processes, procedures, and directives, both public and private? To what extent do base-level units perform cyber mission assurance activities and what factors influence their efforts? The research questions were answered through a comprehensive literature review, and the development and use of a survey.

The research identified the presence of minimal regulatory requirements and a need for consistent guidance, policy and procedures. It also identified trends at units with the task of providing services. The culmination of this effort was the identification of several challenges facing researchers and data from base-level units relevant to the discussion.

Acknowledgments

I would like to express my sincere appreciation to my research chair, Dr. Michael Grimaila, for his guidance and support throughout the course of this effort. I'd also like to thank Dr Robert Mills for his role as academic advisor, teacher, and mentor throughout the program. The insight and experience from both was certainly appreciated.

I would also like to thank Brig Gen David Cotton for his support in distributing the survey created for this project. Additional thanks goes to Terence Sampson who provided the technical work for the on-line survey. I am grateful to both for their support.

I am also indebted to my colleagues in the Cyber Warfare program whose insights and opinion broadened my understanding of the material. Their sense of humor also made the year fly by. Finally, I'm indebted to the many professionals and friends who provided their opinion and suggestions and humored me by lending a sympathetic ear as I endeavored to complete this project.

Maj Mickey R. Evans

Table of Contents

Page

Page

List of Figures

List of Tables

AN INFORMATIONAL ANALYSIS AND COMMUNICATIONS SQUADRON SURVEY OF CYBERSPACE MISSION ASSURANCE

I. Introduction

Nearly every aspect of the military's operations is supported by critical mission systems. Advances in technology has increased the likelihood of success on practically every weapons system and increased the margin of safety for military men and women. As the United States military's reliance on information technology increases, so does the likelihood that the ability of an organization to perform their core mission functions is directly dependent on a service providers' ability to provide basic Information Technology (IT) services.

The need to ensure IT services are available 24 hours a day, seven days a week, 365 days a year is clearly evident, but this is no arbitrary task. It would be difficult to find anyone who would counter the need to provide reliable IT services, yet it would be equally as difficult to find a clearly defined and universally adapted strategy for accomplishing the task. Unfortunately, mission assurance, of any flavor, is often seen as one of those tasks that can take a back seat to more pressing matters such as the daily maintenance and operations of the network. Until an event arises that stresses the day-to-day operations and threatens to jeopardize the Air Force's ability to fly, fight, and win, there never seems to be enough money, time, or manpower to address mission assurance. And when an event does arise on the network, a post event hot wash focuses on the specific IT event and not the broader picture; namely, identifying what impact the event had on operations.

There are several factors which make mission assurance, and in particular, cyber mission assurance planning difficult. Complexities inherent in the problem set (e.g., how do you identify which mission the packets going through the network support); a lack of automated tools (to address the complexity); and an organizational structure in constant flux with undefined lanes in the road. In addition, the lack of standard definitions; a hodge-podge of directives and policies that give lip service to the notion of mission assurance but provide very little if any direction; a lack of accountability; and over-tasked and undermanned units that are just able to make it through the day much less expend energy on planning for something that may never happen.

Where there is a trace of mission assurance activities in the IT field, it is often focused solely on the IT systems themselves, not on the missions they support. The notion of 'cyber mission assurance' is to some extent a misnomer. What good is the most robust of IT systems if, in the end, the missions they support are ineffective? Cyber mission assurance therefore, is a sub-set of an overarching mission assurance effort. Mission assurance, in order to be effective, must address all aspects of the mission, including the role played by cyberspace and the systems that define the domain.

This paper will examine these factors and others in an effort to provide a clear picture of the current state of mission assurance efforts and pertinent directives and guidance. It will also present the results of a survey, aimed at base-level communications squadrons; the goal of which is to provide a snapshot of the realities faced by these units involving cyber mission assurance. Finally, it will present some thoughts and ideas of how some of the current issues can be addressed.

Research Objectives

This paper will attempt to take both a big picture look at cyber mission assurance and a more microscopic look at one functional area in an attempt to link the impacts of one to the other. The big picture view will lead to an examination of current doctrine and policy governing mission assurance in the military. It will also examine current philosophies and accepted standards and methodologies in the commercial sector.

The microscopic look will examine how cyber mission assurance is viewed in a typical base-level communications squadron. More specifically, that portion of the base-level communications squadron that provides core IT functions will be studied. This examination will reveal current thoughts, trends, and actions taking place today at the fundamental level of cyber mission assurance efforts.

Finally, this paper will summarize the current state of efforts, provide suggestions for overcoming difficulties, and provide recommendations on a way ahead.

Methodology

Two types of methodology were employed to produce this paper. The first, involved a thorough review of strategy, guidance, and processes available to both the military and civilian businesses. This also included a review of recent and ongoing research efforts focused on cyber mission assurance. The goal of the review is three-fold, the first is to identify the current state of mission assurance efforts with a focus on cyber mission assurance. The second is to connect the dots with respect to guidance and instruction from enacted legislation to tactical level implementation. The third and final goal is to identify trends in the civilian sector that have potentially beneficial applications in a military environment.

The second method takes the form of a survey; the goal of which is to capture unit level perceptions and opinions concerning cyber mission assurance efforts for communications units. The survey examines unit views of their own mission assurance efforts as well as that of their base and the Integrated Network Operations and Security Center, from which they receive services. It also queried units on their service interruption history, funding, and perceived barriers as they pertain to mission assurance.

Throughout the course of this paper, challenges will be explicitly identified. At the end, these challenges will be gathered and presented.

Background

Much has been written and discussed regarding the vital role information technology plays in today's war fighting efforts. The esteem with which IT has been regarded has grown to the point where it's manifestation as 'cyberspace' has been identified as the newest warfighting domain.

The increase in prestige is a result of IT's contribution to the fight, from the very tip of the spear, all the way back to the most mundane of support activities. Unfortunately, the ability to capture the importance of any given node of the network in terms of its contribution to any specific mission is virtually non-existent. If asked, most IT personnel will respond to questions regarding mission assurance in terms of redundancy and backups. While these are important, the inability to link specific IT assets with their contribution to mission success is a fundamental flaw and the primary barrier to true cyber mission assurance.

It is impossible to talk about mission assurance without talking about risk. A fundamental concept in any mission assurance effort is the need to identify risk and

mitigate threats that could negatively impact the success of a given mission. Readers of this paper should keep in mind that all references to mission assurance and cyber mission assurance presume the inclusion of risk analysis as a part of the process.

Just as it is impossible to talk about mission assurance without talking about risk, it is likewise impossible not to talk about concepts such as disaster recovery, business continuity, and continuity of operations. While it will be established that confusion of these terms is part of the problem, the activities behind the terms provide a foundation for cyber mission assurance. For example, a Continuity of Operations Plan is a key component of a communications squadron's ability to perform its daily mission if and when a catastrophic event unfolds, which in turn provides input to a larger mission assurance strategy.

Standard Definition/Problem Statement

The cornerstone of any endeavor is the premise that there exists a shared, widely accepted foundation on which a standard lexicon can be built and referenced. Unfortunately for mission assurance, such a standard has eluded the commercial and military community. Both the definition of 'mission assurance' and the identification of the very missions we endeavor to secure have evaded our grasp.

It should come then, as no surprise, that a part of the fundamental problem with mission assurance planning is the absence of a standard definition and the undisciplined use of synonyms and phrases. The absence of a standard definition for 'mission assurance' has hindered progress. Many organizations have tried to establish a standard, however communities of interest have failed to adopt a universally accepted definition which has led to miscommunication and ambiguity. Many organizations have assumed

their ‘risk management’ process is the same thing as ‘mission assurance,’ and to be fair, it may be. But for most, they are very different endeavors.

Likewise, the term ‘mission assurance’ is often used interchangeably with phrases such as, ‘continuity of operations planning,’ ‘contingency planning,’ and ‘business continuity [1].’ However, these terms do not mean the same thing to the same people and assuming that they do is a fallacy that has presented obstacles for basic advances in implementing a comprehensive mission assurance strategy.

On 14 January, 2010, Department of Defense Directive 3020.40, ‘DoD Policy and Responsibility for Critical Infrastructure’ was released with a formal definition of ‘mission assurance.’ The full definition states:

> *“A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the Department of Defense to carry out the National Military Strategy. It links numerous risk management program activities and security-related functions, such as force protection; antiterrorism; critical infrastructure protection; IA continuity of operations; chemical, biological, radiological, nuclear, and high explosive defense; readiness; and installation preparedness to create the synergy required for the Department of Defense to mobilize, deploy, support, and sustain military operations throughout the continuum of operations.”* [2]

Challenge #1: Develop a common lexicon for mission assurance linked to the strategic, operational, and tactical levels.

Defining mission assurance in the larger construct is a good first step but more needs to be done. Tailored definitions for communities of interest such as ‘cyber mission assurance’ would go a long way. Standardizing the components of mission assurance

would also be beneficial. Additionally, linking strategic definitions, as in the one above, to tactical level efforts via intermediate levels of standards and definitions is also needed.

Also of note, as it relates to cyber mission assurance, is the difficulty in identifying, and therefore defining the mission to which cyber mission assurance efforts are directed. To illustrate the problem, take the mission of a standard communications squadron. It may be quite easy to identify the mission as defined by the unit. These missions are inherent in the function of the squadron and are somewhat easily identifiable by those within the unit. But what is more relevant, and much harder to define, is the bigger mission as defined by the wing, tenants, MAJCOM, etc. At any given time, data for many missions are traversing IT systems without the knowledge of those responsible for maintaining the system. Figuring out how to conduct cyber mission assurance for the corresponding missions will be quite difficult.

Challenge #2: Cyber mission assurance is cross functional. One has to look beyond the communications unit.

The ability of the communications squadron to effectively plan and execute cyber mission assurance processes for their mission set is important for the unit, but it's only a part of the larger problem set when looking at mission assurance from a higher level in the service or DoD organizational structure. Getting a sortie in the air requires effort from a large cross section of units and requires mission assurance efforts across the spectrum.

Development of Tools

Challenge #3: Develop tools that can map network topology to mission requirements and mission impact.

Unlike the other domains, cyberspace is constantly evolving. Every new device, domain, and subnet effectively changes the landscape. As a result, the ability to create and maintain a view of cyberspace is overwhelming. Adding to the difficulty is the dynamic nature of IP routing. The technology that makes networks function so well, is also partly responsible for making it so inherently difficult to map. The router through which a given mission's data is routed today may not be the same router through which a similar mission is routed tomorrow. Look at a pictorial representation of a network and you'll most likely encounter the ubiquitous 'network cloud,' the space that is undefined, but critical.

If one were to view a mission as a two sided coin with the IT provider on one side and the entity conducting the mission on the other side, one can start to see the dilemma. The communications experts on one side of the coin can't identify which missions will be impacted if a certain router or piece of equipment becomes inoperable. Likewise, the operator on the other side of the coin will be unable to identify which network nodes mission critical data is traversing. Expand this concept beyond the boundaries of a given installation and out to the global Internet and the situation becomes even more complicated.

The combination of the evolving nature of cyberspace, and the dynamics of network routing, results in an environment that is beyond the capabilities of the human

mind to manage. Therefore, there is a huge need to research and develop tools that can do the work for us. Research currently underway by Anderson et al. [3], D'Amico et al. [4], Hale et al. [5], Haigh, et al. [6], and Musman et al. [7] may result in advances in this area. In addition to tools to manage the domain, there exists a need to develop tools to monitor the status of the domain, with the ability to monitor the effects on the missions using the resources. These tools also need to be able to provide their tactical-level status up the chain to higher echelons.

II. Literature Review

To begin to understand where one hopes to go, one must first understand where they are. To this end, both literature from private and public entities was researched in order to identify the existence of standard cyber mission assurance processes or procedures and accepted methodologies. Additionally, information available from public or commercial organizations was reviewed with an eye towards the utility of practices that may be successful in military organizations.

Commercial/Private Sector

In generalized terms, commercial entities seem to have made more headway with mission assurance and cyber mission assurance standardization. This could be attributed to the ease with which these businesses can tie mission assurance efforts and expenditures to the proverbial bottom line.

Although every effort was made to identify and gain access to available literature, limitations were prevalent, mainly in the form of access and discovery. However, given those limitations many resources were available. Among the most relevant were COSO, ITGI, ITIL, and ISO and it is on these processes attention was focused.

COSO

In existence since 1985, the Committee of Sponsoring Organizations (COSO) is a voluntary private-sector organization [8]. Its original function was as a sponsor of the National Commission on Fraudulent Financial Reporting which studied fraudulent financial reporting and the factors that influence such behaviors. Since its inception, COSO had morphed into an organization that provides guidance on such things as fraud,

business ethics, financial reporting, internal controls, and enterprise risk management. COSO is an organization recognized world-wide and is highly respected.

In 1992, COSO published a framework for risk management. It reopened the framework for modification to take into consideration the many changes that have happened to include new rules and regulations as a result of the Sarbanes-Oxley Act of 2002 [9] [10]. The enterprise risk management facet of the COSO framework is pertinent to the cyber mission assurance discussion. COSO recognized the importance, and lack of guidance, of risk management and enlisted the aid of PricewaterhouseCoopers in 2001, to develop the framework to assist managers with efforts to evaluate and improve enterprise risk management. The resulting document, '*Enterprise Risk Management – Integrated Framework'* was subsequently released and is widely recognized as a 'best practice' for risk management [11]. Although the guidance provided by COSO's documents is primarily targeted at the financial sector, they make valid points for consideration by the military. Particularly for ERM, worth noting is the definition:

> *"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."* [12]

As will be seen later in this document, this definition comes close to that supplied by DoD documents to define mission assurance. One negative effect of COSO is that it contributes to the lexicon problem previously discussed. COSO uses ERM and mission assurance interchangeably with detrimental effects.

COSO also explicitly recognizes the critical role of information technology in business functions. In other words, for businesses to succeed, not only should they have

a strategy for their core revenue streams, but also one that includes strategies for the supporting IT assets. For COSO, the recognition was aimed at financial institutions but that can and should be expanded to the military as well. Fortunately, the creation of 24th Air Force and USCYBERCOM is helping to alleviate this problem.

ITGI

The IT Governance Institute (ITGI) was created in 1998 to advance international thinking in standards and governance for IT management. They coordinate a robust mix of international experts, advisors, and contributors to develop their processes. ITGI is internationally recognized as a leader in IT governance and their methods have been used by the Department of Veterans Affairs [13], the US House of Representatives [14] and Sun Microsystems [15].

Control Objectives for Information and related Technology (COBIT) is a product of ITGI. Its stated purposes is to:

> *"provide good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's good practices represent the consensus of experts. They are strongly focused more on control, less on execution. These practices will help optimise IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong."* [16]

COBIT provides two points worth further exploration. One is the use of the words 'ensure service delivery' in COBIT's purpose statement above. In this context service delivery is synonymous with mission assurance. Keep in mind that the 'mission' of a business is to provide its product to the consumer. From this vantage point one can now consider how COBIT could be used by the military when evaluating the way ahead for mission assurance.

The other point is that COBIT provides a mechanism to link business objectives to the underlying IT processes, and hence the IT resources. Again, for a commercial enterprise this linkage means something different than it does to a military organization. However, the methodology employed to show the connections has potential value for the military's cyber mission assurance efforts. In today's technologically advanced military, there is no doubt of the importance of IT. What is difficult is providing the link between operations (business objectives i.e. mission) and IT investment (IT resources). Establishing this link will be key to obtain funding for cyber mission assurance efforts. Funding will be needed to improve the mission assurance posture and COBIT may provide a mechanism to illustrate the benefits to those who control the budgets.

ITIL

The Information Technology Infrastructure Library (ITIL) grew from a set of guidelines published in the United Kingdom in the late 1980s [17]. Recognizing the growing field of information technology, the United Kingdom's government set forth to define a set of standards to be used by government agencies and private sector contractors. The standards are now published under the United Kingdom's Office of Government Commerce as a series of books and have garnered wide spread adoption beyond the UK's government [18].

One of the ITIL books, 'Service Delivery' includes guidance on 'IT Service Continuity Management' which is defined as:

> *"the processes by which plans are put in place and managed to ensure that IT Services can recover and continue should a serious incident occur. It is not just about reactive measures, but also about proactive measures - reducing the risk of a disaster in the first instance."* [19]

This process focuses on recovery from an event that disrupts normal day-to-activities. While this is a vital effort for any business, it does not help to further the notion that mission assurance is more than disaster recovery.

Recognizing the need for continuity to be viewed from a broader lens, the British Standards Institute released an independent standard for 'Business Continuity Planning.' What is significant about this standard is that when completed, it results in a formal printed manual available for reference before, during, and after disruptions [20]. While providing a great resource for business continuity, it does not fully provide a mission focused methodology. Moreover, it does not provide unit level organizations with a standard methodology to conduct continuity planning which will be beneficial to cyber mission assurance efforts. Despite its shortcomings, this could reasonably provide the military with a tactical level model from which to build a tiered process that covers the tactical, operational, and strategic levels.

Challenge #4: Mission Assurance planning, to be effective, must be documented, tested, and operational.

ISO

The International Standards Organization (ISO) is a network of the national standards institutes of 159 countries, with a Central Secretariat in Geneva, Switzerland, that coordinates the system [21]. ISO maintains a repository of 17,000 standards covering everything from agriculture to medical devices to information and communication technologies.

In 2007, ISO published the first internationally ratified benchmark for incident preparedness and operational continuity management, ISO/PAS 22399:2007, *Guideline for incident preparedness and operational continuity management***,** based on the best practices gathered from the national standards of five countries (including the United States) [22] [23]. ISO also released ISO/IEC 24762:2008, *Guidelines for information and communications technology disaster recovery services,* in 2008. Although they do not provide the cross-functional scope needed for mission assurance planning, they are important in that they provide internationally agreed upon and established standards from which to build.

The organizations and standards, summarized in Table 1 which were presented in this section, are not meant to be all-inclusive. Rather, they are a representation of the major influences on the commercial sector towards cyber mission assurance planning. Many companies have established their own processes and procedures, some utilizing the guidelines mentioned, others branching out on their own to do what is best for their company.

Table 1: Summary of Commercial Processes Relevant to Mission Assurance

Organization	Date of Publication	Significance
COSO	1992 Updated 2004	Explicitly recognizes the critical role of information technology in business functions.
ITGI	1996 Updated every 3 yrs	Provides a mechanism to link business objectives (i.e. mission) to IT resources.
ITIL	2001	Process results in a formal printed manual available for reference before, during, and after disruptions.
ISO	2007	Published 1st internationally ratified benchmark for incident preparedness and operational continuity management.

Federal/DoD

The focus now shifts to federal standards and generally accepted practices and procedures. Unlike in the private domain where guidance is typically not regulatory, public agencies are compelled to follow federal mandates. Therefore, what follows is a waterfall review of federal guidelines (where they exist); where one regulatory document influences the ones below.

At the highest level, there have been multiple pieces of legislation which have been passed in an effort to ensure federal systems are prepared to survive and/or rebound from adverse events which disrupt day-to-day operations. With few exceptions, the legislation has viewed information systems as stand-alone entities. That is to say, the legislation has focused on the continuity of the *information system*, not the continuity and success of the missions they support. Even so, the legislation helps to establish a foundation for future cyber mission assurance growth and advancement.

Prior to 2002, diverse pieces of legislation were passed in regards to information technology. Going back three decades, The Computer Security Act of 1987 required the creation of computer security plans to protect sensitive information [24]. The Paperwork Reduction Act of 1995 [25] and the Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act) emphasized a risk-based policy for security continuity [26].

Though well intended, these laws were written at a time when the risk posed by the dependence on information systems was not well understood, nor was the threat. But even so, they are proof that decades ago there began what is an ongoing struggle to

secure and therefore ensure the continuity of information systems with a true cyber mission assurance strategy as the end state.

FISMA

The Federal Information Security Management Act (FISMA) of 2002, requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the data and the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source [27]. The act stipulates that agencies provide, "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency [27]." As a federal mandate, all federal agencies are obligated to comply with its regulatory requirements.

FISMA therefore, is the overarching regulatory guidance for all federal systems, including the DoD.

OMB

To reinforce FISMA, the Office of Management and Budget released Circular A-130 III, *Security of Federal Automated Information Resources.* The stated purpose of the document is to:

> *"establishes policy for the management of Federal information resources. OMB includes procedural and analytic guidelines for implementing specific aspects of these policies as appendices."* [28]

The circular provides that all federal information systems have security plans, requires systems to have formal emergency response capabilities, and requires regular review and improvement of contingency plans for the system be performed.

NIST

As a non-regulatory arm of the Department of Commerce, the National Institute of Standards and Technology (NIST) establishes standards and guidelines used for public and private activities [29] . NIST aims to fill the gap when regulations or laws levy requirements for which there is no, readily available, commercial industry standards.

NIST establishes standards for federal computer systems and releases them in Federal Information Processing Standards (FIPS) [30]. Unlike the standards developed for commercial enterprises, FIPS are compulsory and binding for federal agencies. NIST, through its Information Technology Laboratory, also publishes guidance documents and recommendations in a series of special publications.

In response to FISMA and the OMB Circular, NIST developed the FISMA Implementation Project consisting of two phases:

-Phase I: Standards and Guidelines Development (2003-2012)
-Phase II: Implementation and Assessment Aids (2007-2012)

Under Phase I, NIST has released several FIPS documents that deal with risk management and security but none that deal with mission assurance. Under Phase II, NIST is providing implementation and assessment reference material for organizations applying the NIST processes. Outside of the FISMA Implementation Project, NIST has also released a series of Special Publication (800 series) aimed at improving contingency planning. These standards, like other documents discussed, treat information systems as a stovepipe and do not address mission assurance from a broader lens.

DIACAP

FISMA is in large part responsible for the requirements Air Force systems face as part of the DoD Information Assurance Certification and Accreditation Process (DIACAP). NSA, as the regulatory arm for DoD Systems below the federal level, uses the DIACAP to ensure DoD systems are incorporating risk management processes into their IT systems. DIACAP institutes a certification and accreditation process to set standards for systems. As a part of that process, systems must have documented contingency plans that are routinely tested [31].

The Air Force has tailored DIACAP to enable its use within the confines of Air Force structures. The Air Force DIACAP is much the same as the overarching defense department process.

The Air Force and DoD use DIACAP to comply with FISMA. Similarly, they have developed reporting structures to report compliance with FISMA back to Congress. The Enterprise Information Technology Data Repository (EITDR) is used by the Air Force to report compliance to DoD which in turn uses the DoD Information Technology Portfolio Repository (DITPR) to report to OMB and then to Congress [1].

Table 2, provides a summary of the organizations discussed and a brief description of the significance it provides.

Table 2: Summary of Relevant Federal/DoD

Entity	Date of Publication	Significance
FISMA	2002	Requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency.
OMB	2000 Revised	Establishes policy for the management of Federal information resources.
NIST	2003	NIST establishes standards for federal computer systems. Developed the FISMA Implementation Project.
DIACAP	2007 Note: predecessor released in 2000	Ensures DoD systems are incorporating risk management process into their IT systems and used by DoD to report compliance with FISMA to Congress.

Current State

As stated before, cyber mission assurance, as a sub-category of mission assurance requires a holistic approach, not stove-piped attempts. Unfortunately, cyber mission assurance efforts have failed to achieve that level of performance and continue to operate, where present, within the confines of their own system. Despite the slow progress being made, many organizations are expending considerable effort to solve the problems.

Office of the Secretary of Defense

In February 2007, the Department of Defense formed a Global Information Grid (GIG) Mission Assurance Working Group to research how the department would be able to perform its mission essential functions if networks were attacked or degraded. The group studied the issue for seven months and in the end, articulated three conclusions [32]:

- DoD fights on a GIG built for business efficiency instead of Mission Assurance against sophisticated threats

- The GIG is fragile and vulnerable to attack
- There is inadequate focus for Mission Assurance in a Net-Centric Environment

The working group went on to provide three suggestions to address the issues:

- Improve the Department's ability to plan, simulate and execute exercises under serious cyber degradation
- Enable situational awareness, improve diversity planning, and integrate policy and plans for network resiliency
- Transform to address assessments, compliance, and measurability focused on mission driven risk management

The results of the working group were briefed to department leaders and a strategy for developing the suggestions was developed and is being put into action.

The working group also developed a cyber mission assurance goal, which states:

> *"Reduce risk of degraded or failed missions by developing strategies, policies, architectures, and by promoting exercises; all of which enhance network resilience, continuity plans, and protect critical information infrastructures."* [32]

The influence of the working group on DoD leadership can be seen when Robert Lentz, the Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance testified before the U.S. House of Representatives Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities on 5 May 2009. During the testimony, when speaking on network resiliency, he quoted from the Department's Guidance of the Development of the Force (GDF) for 2010-2015, signed in May 2008,

> *"All DoD Components will reduce the risk of degraded or failed missions by developing doctrine/tactics, techniques and procedures and planning for, implementing, and regularly exercising the capability to fight through cyber or kinetic attacks that degrade the Global Information Grid."* [33]

The quote and the goal from the working group are remarkably similar.

Challenge #5: Current OSD efforts do not help mission assurance within the boundaries of an installation.

While this effort promises much in the way of advancing the departments mission assurance efforts, it does have at least one drawback. The wiki site for this effort, Network Resilience & Cyber Mission Assurance [32], goes on to state the coordination effort required and mentions US Strategic Command, Chairman of the Joint Staff, and Defense Information Systems Agency including the responsibilities of each. And while there is a place for Military Services, the responsibilities section is ominously empty [32] . Obviously, more remains to be done.

This effort is a great start but falls short of the requirement. Protecting and planning for mission assurance of the Global Information Grid (GIG) is no doubt required. But, this effort does nothing for the organizations working within the boundary of an installation. The GIG presence, as managed by DISA, only goes to the point-of-presence on a base. What happens beyond the point-of-presence (i.e. within the perimeter of an installation) is equally as important. GIG assurance without installation network assurance is ineffective.

Inspections

Challenge #6: DIACAP is not effective.

In 2008, the DoD Inspector General (IG) conducted a review of the department's compliance with FISMA by examining the accuracy of the services' reporting of contingency plans for critical systems identified in

the DITPR [1]. Mission-critical was defined as, " the loss of mission-critical system operations would cause the stoppage or direct mission support of warfighter operations [1]." The IG chose a random sample of 240 of the 436 systems in DITPR and asked DoD components to provide them with a copy of the approved contingency plan for the sampled systems. The report found that, "on the basis of the sample results, 264 of the 436 mission-critical DoD systems did not develop or could not provide evidence of the system's contingency plan." Keep in mind that in order to be a mission-critical system, the system had to go through the DIACAP process which *requires* a contingency plan.

Challenge #7: Leadership is lacking.

Specifically for the Air Force, the IG, "projected that owners of 68 of the 85 mission-critical information systems (80 percent) did not develop or could not provide evidence of a contingency plan [1]." They also found that 100 percent of the systems did not test or could not provide evidence of testing the contingency plan.

The IG report highlights two other problems that have department wide ramifications for cyber mission assurance. The first is that the,

> *"ASD(NII)/CIO did not establish a comprehensive and overarching contingency planning policy. Further DoD Component CIOs did not implement management controls to verify that system owners developed and test system contingency plans as required or to support the assertions in their CIO Certification Memorandums about the completeness and accuracy of their information in DITPR.* [1]*"*

The report went on to suggest that the ASD(NII)/CIO should either require the DoD components to implement NIST Special Publication 800-34 or issue a comprehensive policy for contingency planning.

The second is that the DITPR Data Dictionary is confusing by using terms such as 'contingency planning' and 'COOP' interchangeably when in fact they have separate meanings. This reinforces observances made earlier in this paper.

Historically, those tasks upper echelons of the military organization identify as important, inevitably find themselves as the focus of an inspection and are routinely scrutinized for their compliance with standards. Due to a lack of standards by which to measure, it should come as no surprise that a unit's ability to provide cyber mission assurance is not inspected.

A quick search through AFI 90-201, Inspector General Activities [34] will result in no inspectable areas containing 'mission assurance' at unit level that are inspected. There is one item for Component –Numbered Air Force readiness inspections (C-NAF includes the Air Force Forces staff, the commander's support staff, the Air and Space Operations Center and specialty teams assigned throughout the C-NAF) in Attachment 2 of the AFI.

Unit

At unit level, the picture is even worse. Units struggle just to meet daily operations and maintenance requirements. There are no guidelines to follow that units can use to implement cyber mission assurance. There are some technical advances such as virtualization, cloud computing, and redundant systems that may help to increase the

chances that systems can continue to support the mission. But, these advances do not, in and of themselves, advance cyber mission assurance efforts.

Figure 1, summarizes guidance and the corresponding reporting structure affecting Air Force systems. As can be seen from the figure, guidance stops at the service level, leaving MAJCOM's, and more importantly units, to act on their own. It also shows that reporting is correspondingly performed from the services up to Congress, which as was previously discussed, is horribly inaccurate. Finally, it illustrates that the process is system specific, not mission specific.

	Guidance*	Reporting
Law	FISMA	Scorecard/Report to Congress
Federal	FIPS Pubs	Scorecard to OMB
DoD	DIACAP	DITPR
Service	Air Force DIACAP	EIDTR
MAJCOM	None	None
Base/Unit	None	None

*Reporting is system specific, NOT mission specific

Figure 1: Summary of Federal/DoD Guidance and Reporting

MAAP

The Mission Assurance Analysis Protocol (MAAP) is an initiative that may help to change the way in which the DoD, and therefore the Air Force perform mission assurance. Sponsored by the Department of Defense, MAAP was developed in 2005 by researchers at Carnegie Mellon. It "defines an advanced, systematic approach for

analyzing operational risk and gauging mission assurance in complex work processes [35]."

The MAAP protocol uses the mission to frame risk analysis and allows for the inheritance of risk from other processes that have inputs to the current process. This has the real potential of obtaining the holistic approach that has thus far been elusive. Using MAAP, the possibility exists to link cyber processes to operational processes. It also creates a baseline for showing the inheritance of risk at one level to processes at other levels. The joint nature of warfighting today virtually mandates this type of cooperation to effectively implement mission assurance.

III. Mission Assurance Survey

It is important to set the preceding discussion in the context of current practice. As with most military endeavors, there is the reality of strategy, doctrine, and regulation that provides the black and white sources from which tactical guidance is derived. There are also the realities surrounding the tactical level implementation and the culture and atmosphere under which it takes place.

The research and review of private and public documents discussed so far, regarding mission assurance, provides an academic, and somewhat clinical, view of the current landscape. To truly appreciate the reality of cyber mission assurance at the tactical level requires a different tactic. To that end, an on-line survey was produced, the goal of which, was to provide a snapshot of the current realities and atmosphere for cyber mission assurance efforts at the unit level.

The survey contained 41 questions which asked respondents to provide data involving the current state of mission assurance planning from a base, unit, and I-NOSC perspective, sources of funding for mission assurance planning, and historical incidents which have resulted in disruption of day-to-day operations. It also asked respondents to self-assess their mission assurance activities. Appendix 1 contains a list of the questions and available response options.

Overview

The survey only considered that part of a communications unit that dealt with core IT services. Core services as defined by AFI 33-115V1 are :

> *"those services defined by the Air Force IT community as central components of the AF-GIG. They embody the seamless, secure, and*

reliable transport of timely and trusted information across the AF-GIG." [36]

The specific core services as defined by the AFI are [36]:

-Electronic Messaging
-Address Management
-Directory Services
-Information Assurance and Security Hardware. (Simple network management protocol [SNMP] monitoring and control of:
    1) software
    2) bandwidth
    3) hardware [ports, interfaces, etc.])
-Domain Name Servers (DNS)
-Exchange
-Windows Internet Naming Service (WINS)
-Domain Controllers (PDC/BDC) remote (PDC/BDC)
-Dynamic Host Control Protocol (DHCP) server
-Local Directory Service Agent (LDSA)
-Defense Message System (DMS)

The survey focused on seven specific areas:

-The status of a base/wing mission assurance plan
-The status of a NOSC mission assurance plan
-The status of a unit mission assurance plan
-The existence of conflicts where multiple mission assurance plans exist
-Barriers and Drivers for mission assurance efforts
-Historical events that have threatened the mission
-A self-assessment of the change in mission assurance readiness

Respondent Statistics

With support from SAF/XCT, a message was sent to all MAJCOM A6s asking for communications squadron commanders to complete the mission assurance survey. The on-line survey opened on 18 March 2010 and closed on 31 March 2010. Of the 62 responses received, 60% (37) were from guard and reserve units while the remaining 40% (25) were from active duty units. The majority of the respondents, 52%, were unit commanders. Another 19% were deputy commanders or directors of operations,

operations flight commanders, plans flight commanders, or action officers. 29% identified as 'other.' The average amount of experience in the unit for respondents was 4.48 years. 82% either 'agreed' or 'strongly agreed' that they are 'Personally Very Involved In IT Mission Assurance In [their] Unit."

Base/Wing Mission Assurance

The first focus area concentrated on the base or wing's mission assurance plan. Each wing has a specific mission and just as the communication's unit should be interested in planning for mission assurance, so should the installation on which the communication's unit resides. 39% of all respondents said their base or wing had some sort of a plan for mission assurance in various stages of readiness, as depicted in Figure 2. 31% said the plan was being developed. 30% said there was no plan currently in place.

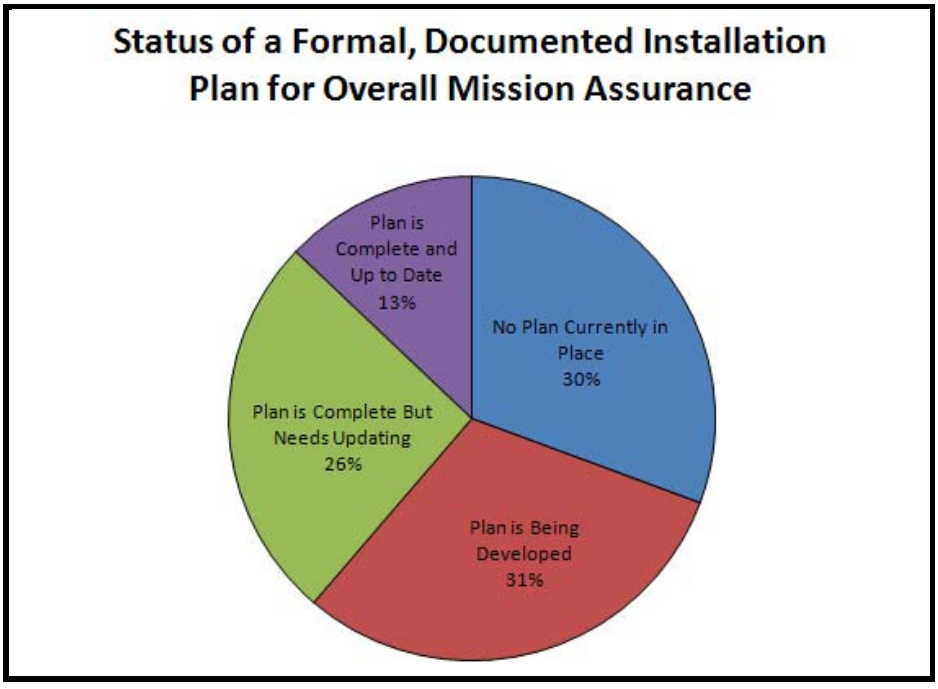

Figure 2: Status of Installation Mission Assurance Plan

The numbers paint a worse picture for active units than for guard and reserves. 46% of active units reported no base or wing plan. On a positive note, 91% of all respondents said that where a base or wing plan existed, IT was included.

The value of any plan is only as strong as the extent to which it was tested and verified. Beyond the basic test, to determine if it meets the desired goal, there exists the need to periodically test the plan to see if it continues to meet the need and to train personnel on its implementation. When asked for the time frame in which the base or wing plan was last tested, 44% reported that the last test had been conducted within the last year, see Figure 3. Nearly as many, 30% (7) could not identify when the last test had taken place. Of the 17 respondents that completed the question regarding the type of activity used to test the base/wing plan, 8 said the test was in the form of a table top

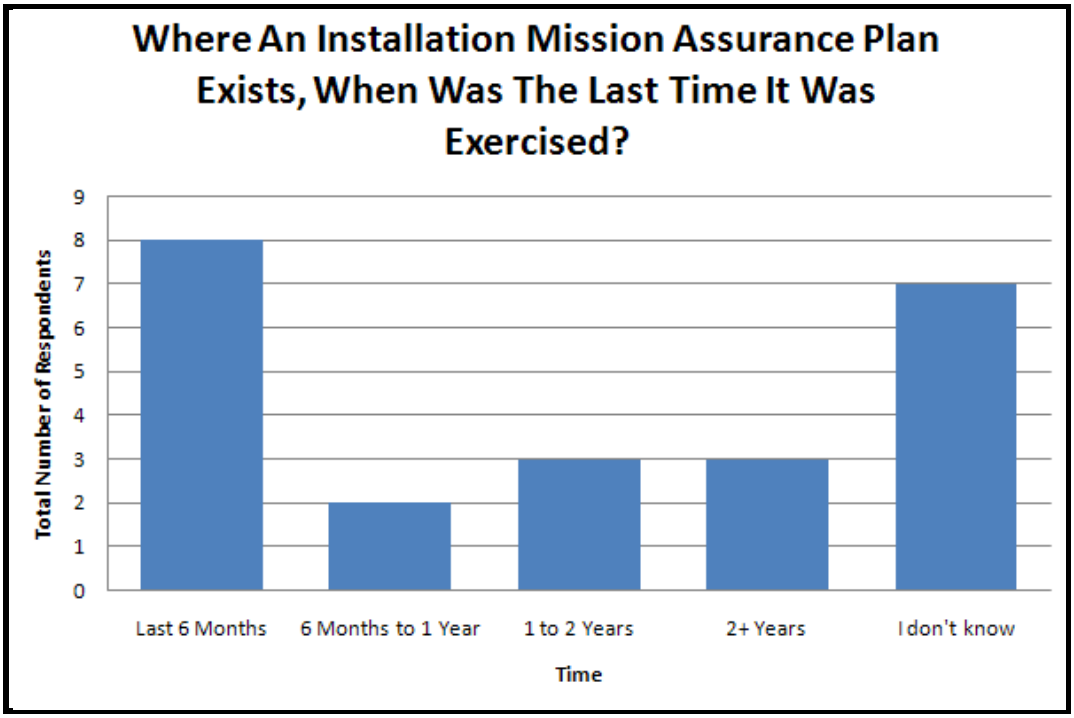

Figure 3: Installation Plan Testing

exercise and another 8 said the test was scheduled in advance (possibly as part of an ORI). Only 1 reported that the test was completely unscheduled.

Finally, as depicted in Figure 4, of the 70% (43) respondents that said there was either a plan of some sort in place or one was being developed at base/wing level, only 56% (24) said that an individual had been appointed at the installation level who was responsible for mission assurance.

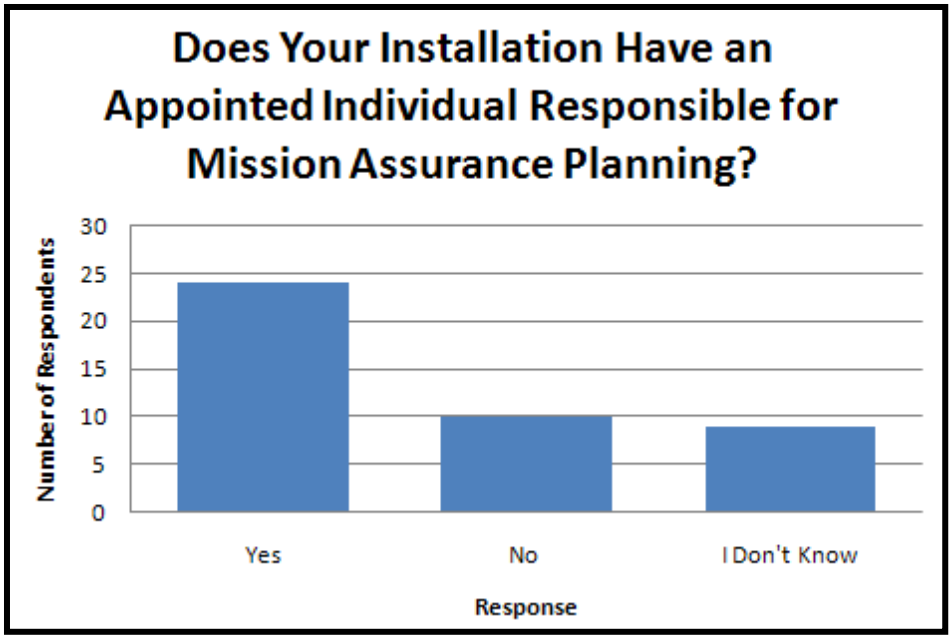

Figure 4: Status of Installation POC

Integrated - Network Operations and Security Center Mission Assurance

The Air Force Network Operations (AFNETOPS) construct is the latest iteration of the way in which the Air Force manages its portion of the Global Information Grid (GIG). Section 4.4.4 of AFI 33-115V1, Network Operations states that

> *"The I-NOSC ensures Air Force networks are capable of conducting, supporting, and advancing coalition, joint, Air Force, and interagency operations. Through a common environment, the I-NOSC provides situational awareness to the AFNOSC, WFHQ, and MAJCOMs. Each I-*

NOSC will oversee the operation of the base level NCCs, while providing remote administration of enterprise-wide infrastructure."

It is important to note, from the definition, that part of the I-NOSC's responsibility is to provide remote administration to the enterprise-wide infrastructure. In short, the I-NOSCs provide services and support to base level communication's units, which is why the base level units have a vested interest in the mission assurance plans of the I-NOSCs.

10% (6 of 62) of respondents reported they do not receive services from an I-NOSC. Four of those were Guard units and one was itself an I-NOSC. The one remaining was an active duty unit. Three respondents did not provide responses on the section of the survey asking details about the I-NOSCs plan, even though they reported that they receive services from the I-NOSC.

What follows is data pertaining to the 85% (53 of 62) of respondents that reported they do receive services from an I-NOSC and provided answers questioning the status of the I-NOSC plan.

Only 24% of the respondents, see Figure 5, said the I-NOSC from which they receive services had some sort of a plan for mission assurance in various stages of readiness. 36% said the plan was being developed. Combined with the 40% that said there was no plan currently in place, 76% of respondents report there is no mission assurance plan in place, at this time, that they could turn to, should an event occur that causes a significant impact in day-to-day operations. When asked if the services they receive from the I-NOSC are covered in the I-NOSC mission assurance plan, only 78% responded 'yes.'

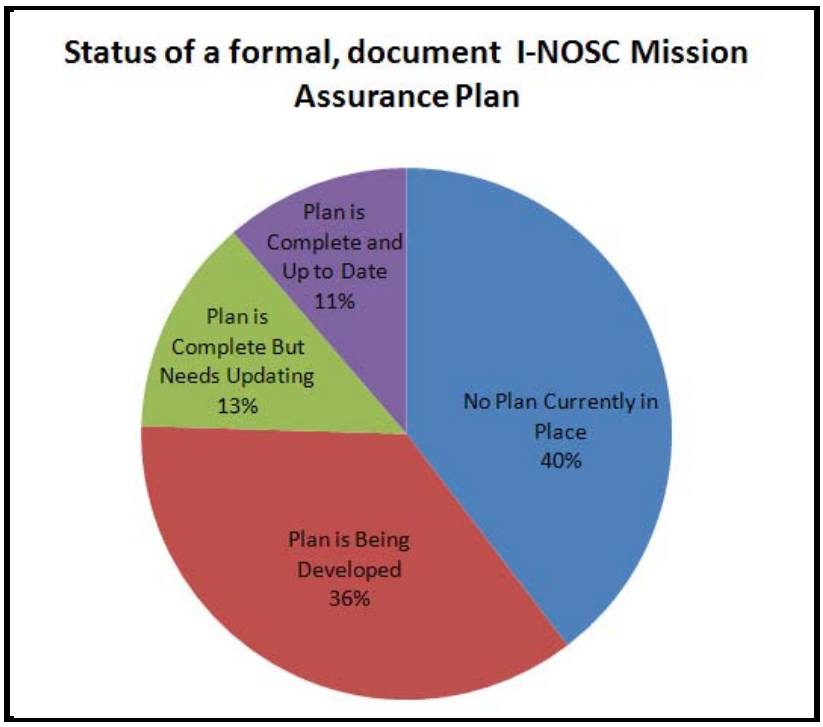

Figure 5: Status of I-NOSC Mission Assurance Plan

As shown in Figure 6, 46% said the plan had been exercised in the last year. The remaining 54% could not identify when the plan had last been tested. Of the 6

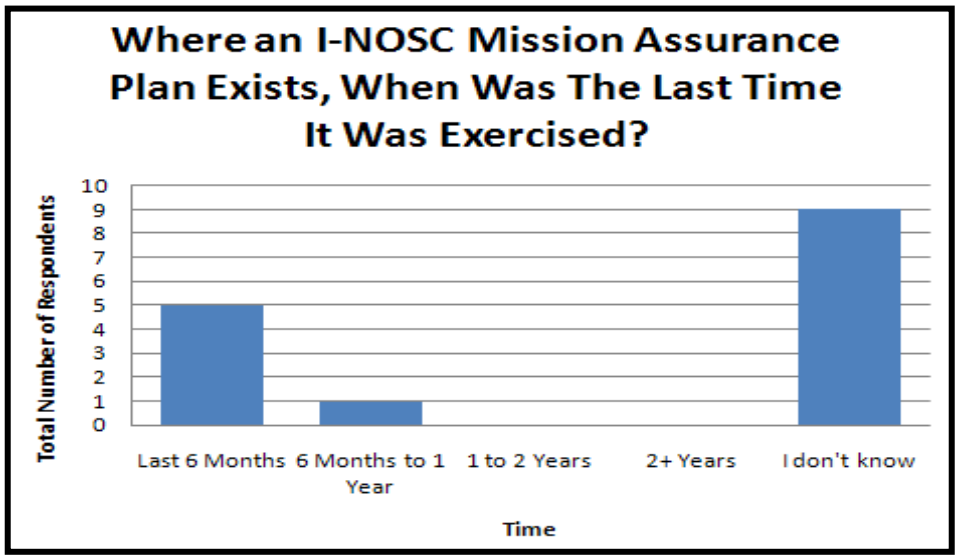

Figure 6: I-NOSC Plan Testing

respondents that completed the question regarding the type of exercise used to test the I-NOSC plan, 5 said the exercise was scheduled in advance. One reported that it was completely unscheduled.

Only 22% responded that there was a POC responsible for mission assurance planning at the I-NOSC level. The remaining 78% said that either there was no POC or they did not know if there was one.

Unit Mission Assurance

45% of all respondents said their unit had some sort of a plan for mission assurance in various stages of readiness. 27% said the plan was being developed with the remaining 28% responding that there was no plan currently in place. Figure 7, shows the number of respondents, broken out but active duty and guard/reserve units and how they

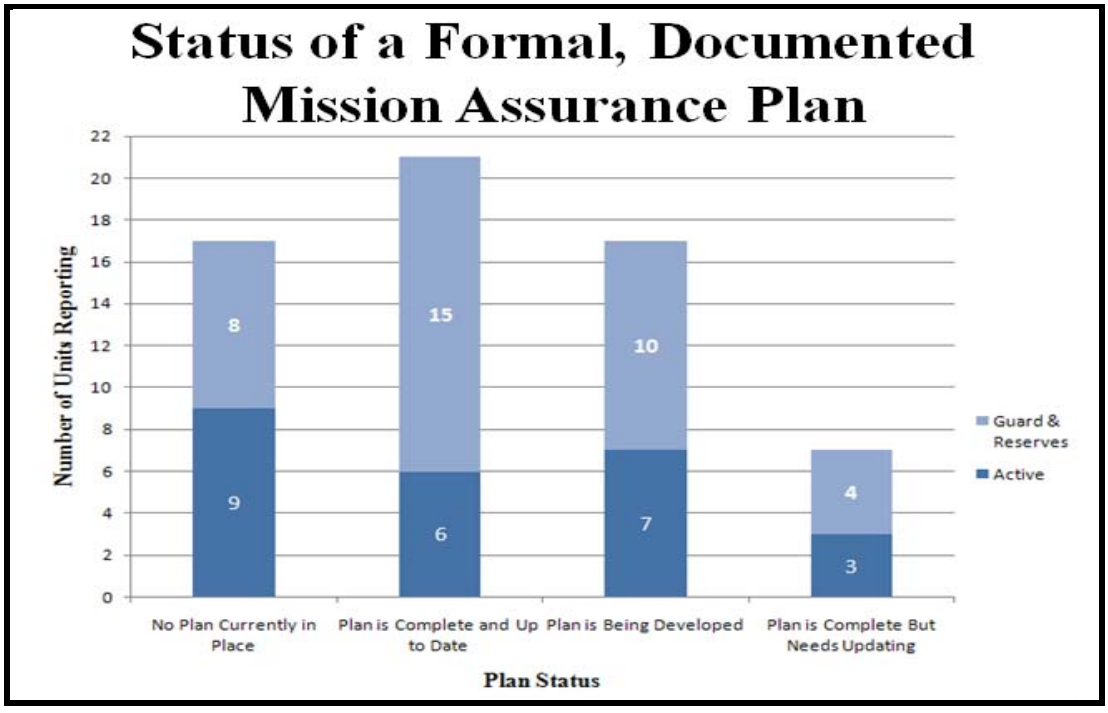

Figure 7: Status of Unit Mission Assurance Plan

responded. The numbers paint a worse picture for active units than for guard and reserves. 40% of guard and reserve units report they have a mission assurance plan that is complete and up to date, only 24% of active duty units reported the same.

When asked for the time frame in which the unit's plan was last tested, 50% of the respondents reported the plan had been tested in the last 12 months. 21% could not identify when the last test had taken place, see Figure 8. Of the 20 respondents that completed the question regarding the type of exercise used to test the unit plan, 8 said the test was in the form of a table top exercise and 9 said the test was scheduled in advance (possibly as part of an ORI). 2 reported that the test was completely unscheduled and the

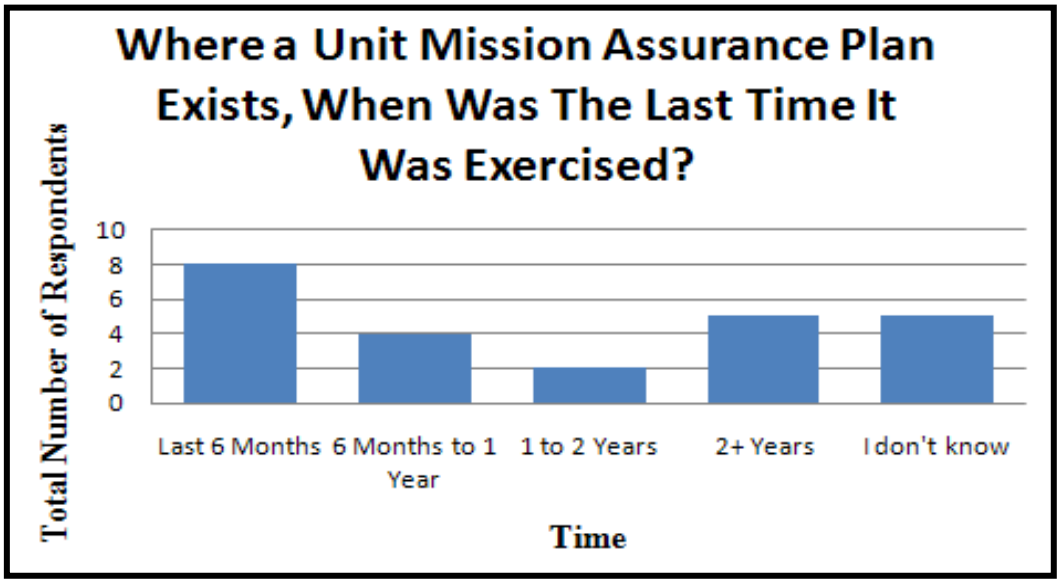

Figure 8: Unit Plan Testing

remaining respondent reported that the type of test fell into the 'other' category.

Of the73% (45) respondents that said there was either a plan of some sort in place or one was being developed at base/wing level, only 67% (30) said that an individual had been appointed at the unit level who was responsible for mission assurance planning.

And finally, of the 45 respondents that reported that a plan was either being developed or existed in some form, only 40% (18) reported they had been contacted to support other units' mission assurance efforts.

Miscellaneous Base-Level Focus Areas

It is clearly evident from the data presented so far that there is a large deficit in the existence of active mission assurance planning throughout. A series of questions was asked to try to develop an understanding of what might be affecting the process. The first questions asked respondents to identify the primary and secondary drivers for mission assurance planning at their base. In other words what, if anything, was motivating the base-level units to engage in mission assurance planning. Figure 9, shows the results.

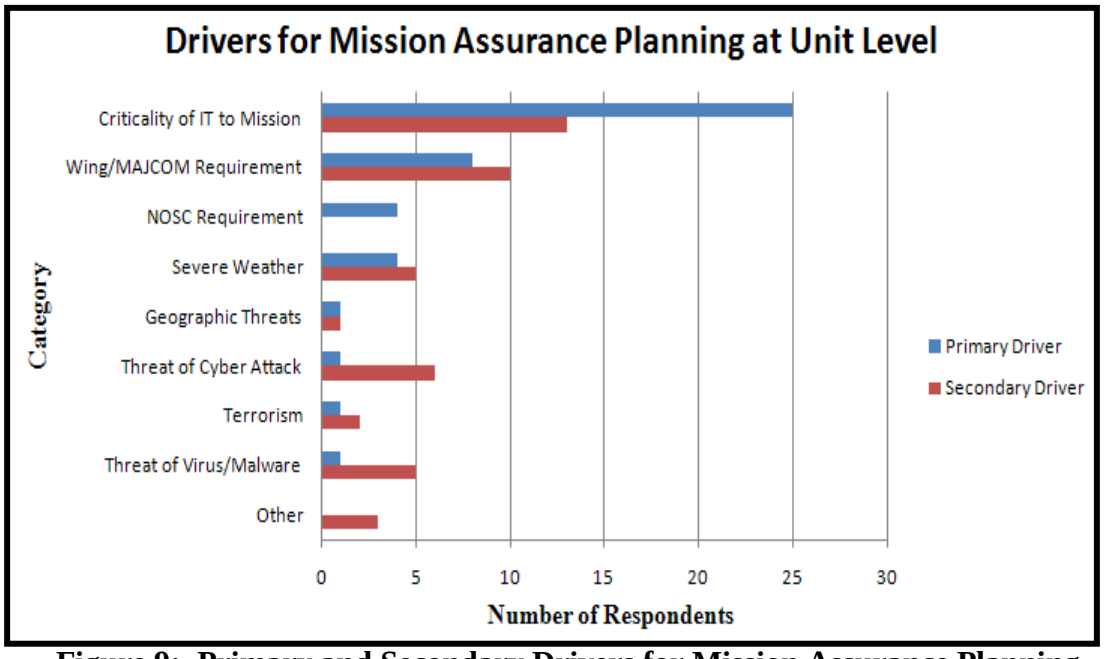

Figure 9: Primary and Secondary Drivers for Mission Assurance Planning

From the data, one can see that the critical role IT resources plays in the mission of the base is by far the main reason units are involved in mission assurance planning.

However, what is surprising is that the second and third reason is identified as a wing/MAJCOM or I-NOSC requirement. In all cases, except one, respondents that identified the presence of a wing or I-NOSC mission assurance plan reported a corresponding requirement from that same entity for their unit. It seems to be evident that base level units are encouraged to develop mission assurance plans when it is also important to either their wing leadership or their I-NOSC. In the case of the lone exception, the respondent reported that the primary driver was the Wing/MAJCOM yet reported that the wing had no plan of their own.

The remaining question asked units to identify the barriers to IT mission planning at their base. Respondents had the option to select up to two responses. Figure 10, provides a summary.

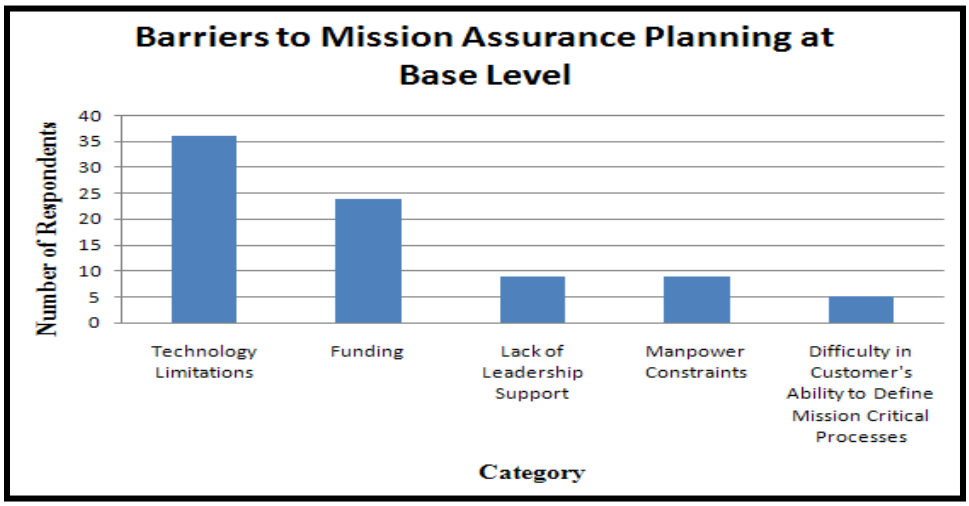

Figure 10: Barriers to Mission Assurance Planning at Base Level

The data shows that the primary barrier is related to technology limitations. The secondary barrier is funding. This correlates to the earlier observation that units are

undermanned and that tools need to be developed to assist with mission assurance planning.

When asked if their unit received funding specifically for mission assurance planning and/or implementation of mission assurance measures, 71% reported that they did not. 3% reported that they did. The remaining, 26% were unsure. This data, along with the data concerning barriers to mission assurance planning suggests that funding, specifically for mission assurance planning, is needed.

Incident History

At its most basic level, mission assurance encompasses the component referred to as continuity of operations. At the foundation of mission assurance is the unit's ability to provide its core functions. Knowing what has happened, from an historical perspective, that caused units to deviate from normal day-to-day operations is relevant in trying to understand where to concentrate efforts that will make the most significant impact on the way ahead. What follows is data resulting from a series of questions regarding the actual incidents that have occurred in the last five years.

Figure 11 summarizes data provided when asked about the number of disruptions experienced in the last five years. 55% of the respondents reported they had experienced at least one incident in the five year time frame. In fact, 10 units reported they had experienced three disruptions. 14 units reported they had experienced five disruptions or more.

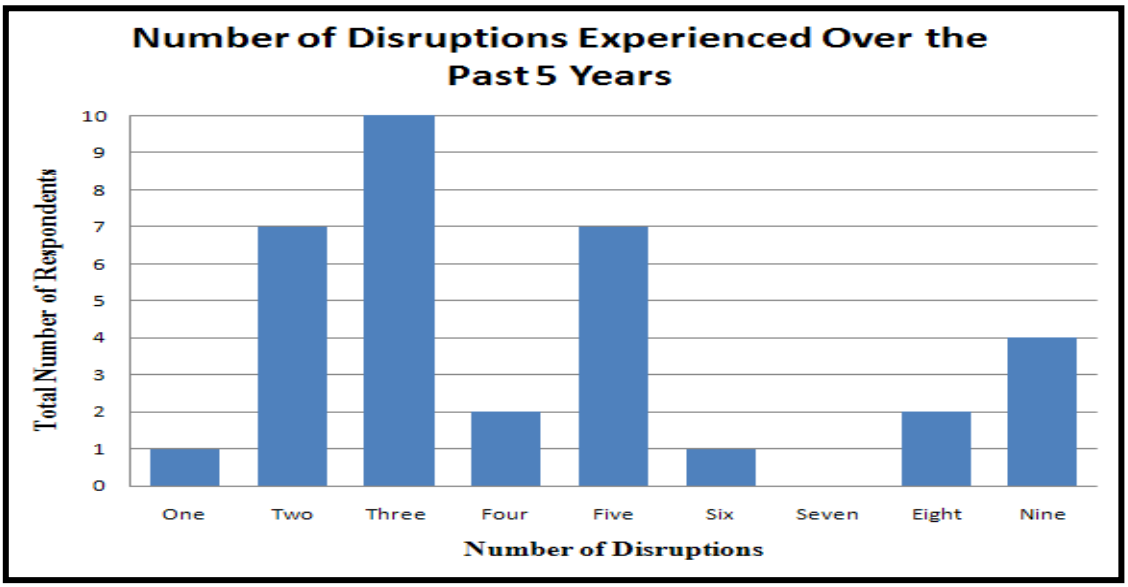

Figure 11: Number of Disruptions in Past Five Years

Respondents were asked to provide additional details on the two most significant disruptions experienced in the five year period, the data is provided in Figure 12. The majority of the disruptions, 75% were caused by one of four factors, electrical, hardware

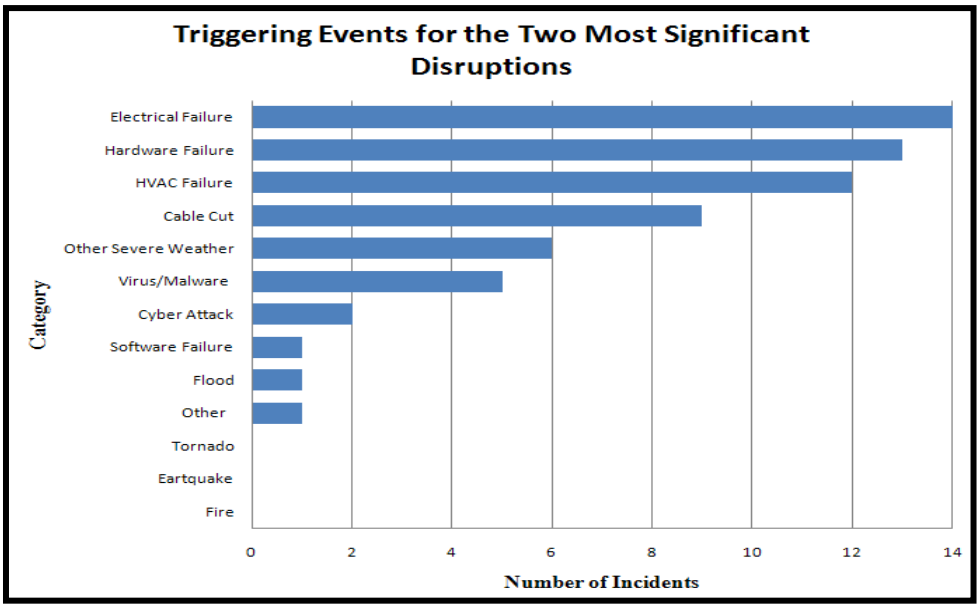

Figure 12: Triggering Events for Most Significant Disruptions

or HVAC failure, or a cable cut. Another 9% was caused by severe weather. 3% (2 responses) reported a disruption that was caused by cyber attack. This label is broad in scope and there was no clarifying data to elaborate on the specific type of cyber attack. In addition to identifying the triggering events for the two most significant disruptions, respondents were asked to identify the consequence or impact of the disruptions; Figure 13 provides a summary of the data. Respondents were not limited in the number of options they could choose; they could select all that apply. 75% of respondents said the impacts manifested themselves in the form of services being unavailable including the network itself, applications, E-mail or web sites. Damage to hardware, software, and data was only reported by 11% of the respondents.

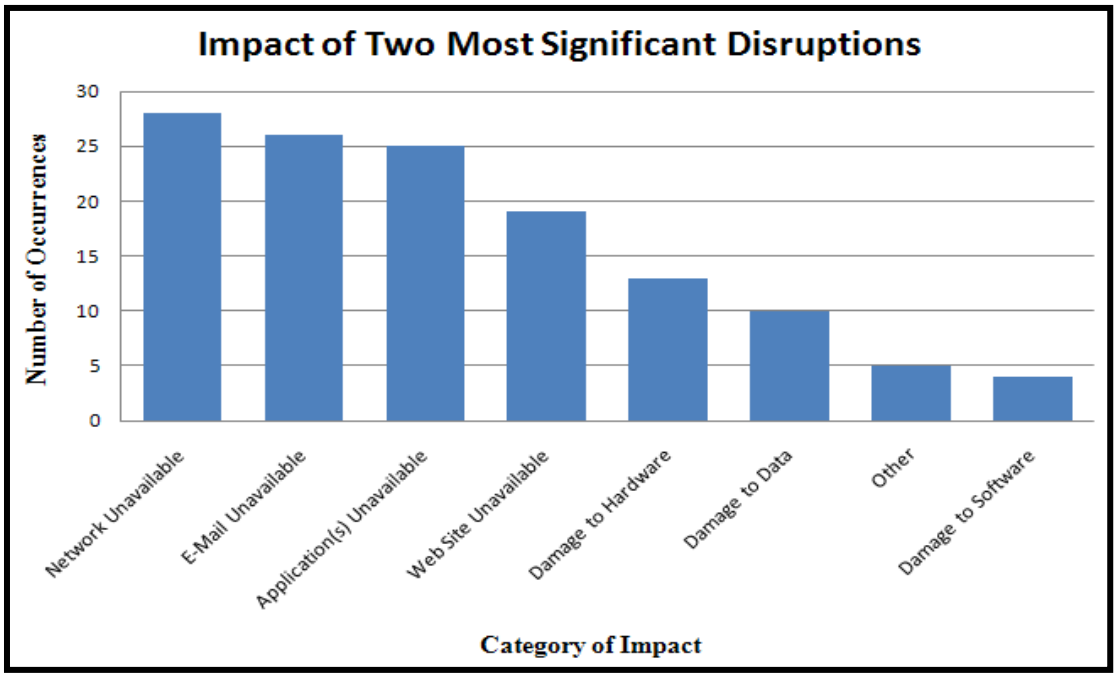

Figure 13: Impact of the Two Most Significant Disruptions

Finally, regarding the most significant event experienced, respondents were asked to assess both the impact of the event and the impact to the base-wide mission. The results of the data are summarized in Figure 14.

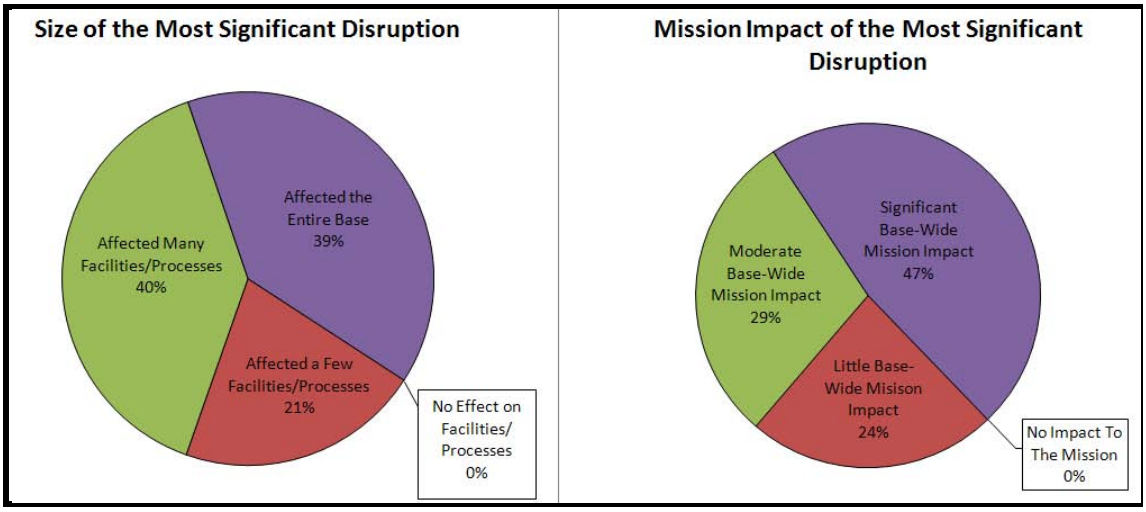

Figure 14: Size and Mission Impact of the Most Significant Disruption

Regarding the size of the most significant disruption, 39% reported that the event impacted the entire base. Another 40% reported the impact was felt by many facilities and/or processes. Only 21% were able to report that there was minimal impact. Based on this data it seems that base-level units struggle with the ability to provide redundant system capabilities and are unable to provide continuity of operations much less mission assurance.

The data reported, for the impact of the most significant disruption on the base-wide mission, is also impressive. 76% of respondents report that the impact either affected the entire base or many facilities and/or processes. Only 24% reported that there was little base-wide impact.

Self Assessment

The final series of questions on the survey asked respondents to identify the importance of IT to the missions of other units on base, self assess their unit's ability to restore mission critical systems today, compare that ability today with two years ago, and to rate their mission assurance readiness.

Figure 15 summarizes the data respondents provided when asked to assess the importance of IT to the mission of other units on base. While 68% of units reported

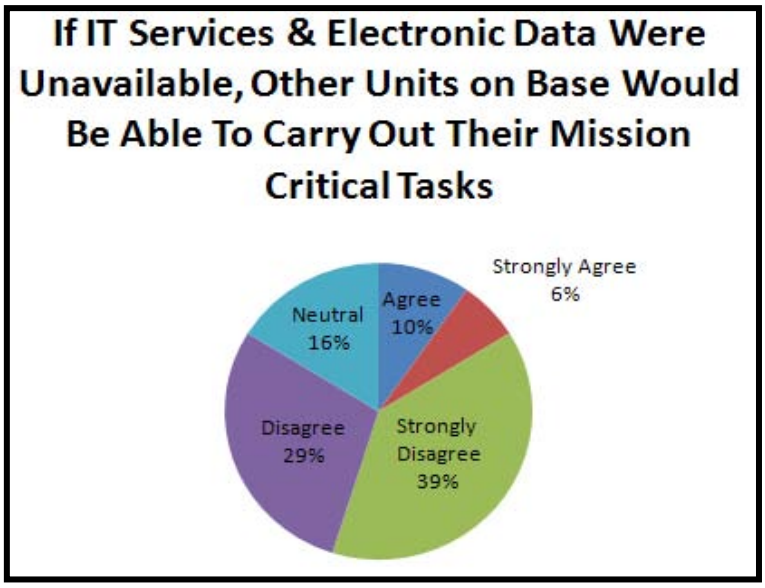

Figure 15: Assessment of Mission Impact of Availability of IT Resources

they either 'disagreed' or 'strongly disagreed' with the statement, "If IT services & electronic data were unavailable, other units on base would be able to carry out their mission critical tasks,' 16% reported they either 'agreed' or 'strongly agreed.' These units believe IT is not an essential part of other units' mission capabilities. With the proliferation of IT services today, it is hard to comprehend this piece of data. What is

perhaps more troubling is that 16% were neutral. One could draw the conclusion that for those 16%, they have no concept of what, if any, services they provide that are mission critical to other units.

The next questions asked respondents to self assess their unit by addressing the following question, "My unit is prepared to restore mission critical systems in the event of a disruption." Figure 16 illustrates the data received. 61% of units 'agreed' or 'strongly agreed' that they could restore mission critical systems. That leaves 39% of respondents that were either neutral or believe they could not restore mission critical systems in the event of a disruption. This data is daunting for those missions that depend on IT services.

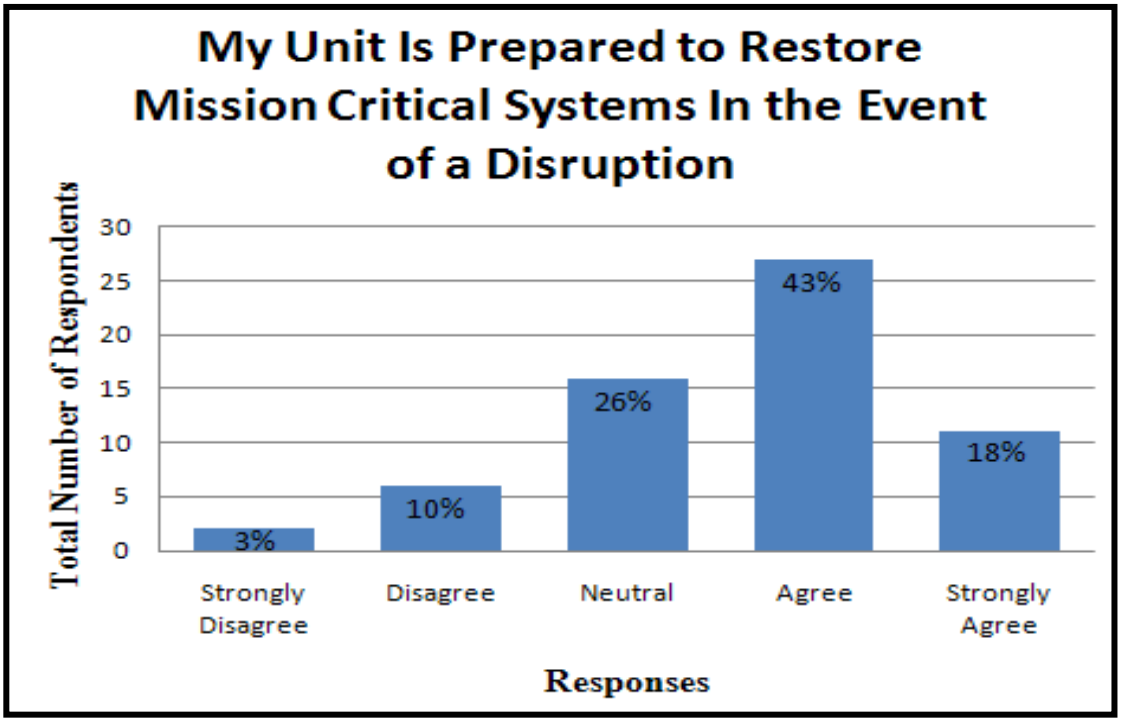

Figure 16: Self-Assessment of Units' Ability to Restore Systems

Next respondents were asked to rate the level to which they agree with the following statement, "My unit is better prepared to restore mission critical systems today than it was 2 years ago," see Figure 17. 69% agreed, to some level, with the statement. Another 25% disagreed, to some level; meaning they assess their ability to deal with adversity has gone done over a two year period. Obviously more analysis than provided

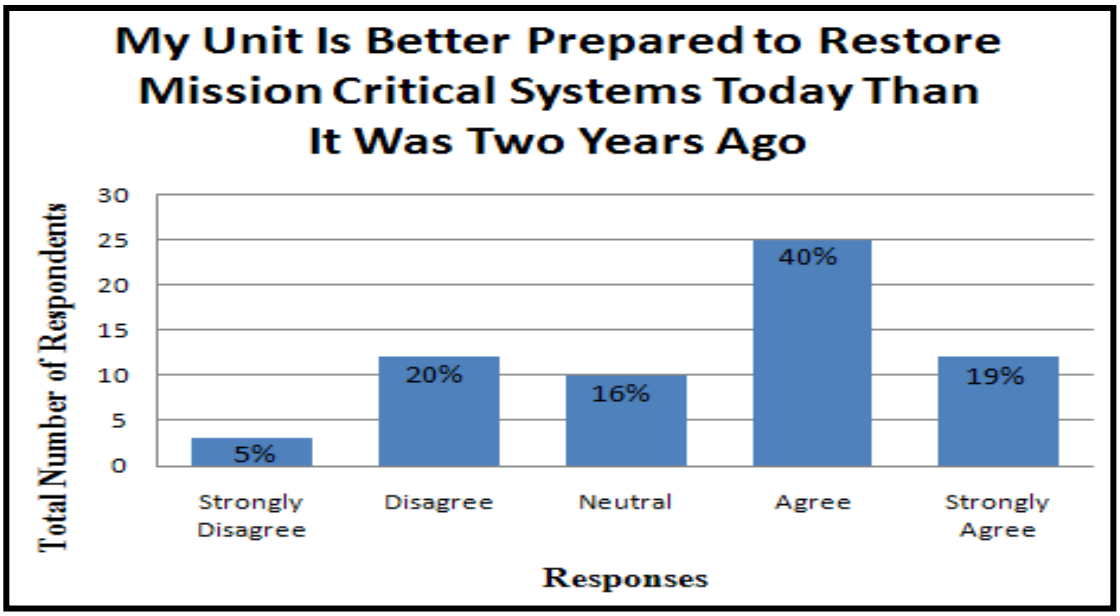

Figure 17: Self-Assessment of Units' Ability to Restore Systems Today Compared to Two Years Ago

by this survey would be needed to get to the core of the responses but, they are somewhat shocking nonetheless. 16% of respondents reported their ability to restore services had neither gone up or down.

Figure 18 illustrates the findings from the last question, in which respondents were asked to assess the level of performance their unit had achieved in its IT mission assurance readiness. 24% reported their unit was at risk in its ability to provide IT mission assurance. Another 10% were unable to provide an assessment of any kind.

Only 24% self assessed their unit's ability in a positive light while 42% rated their level of performance as adequate.

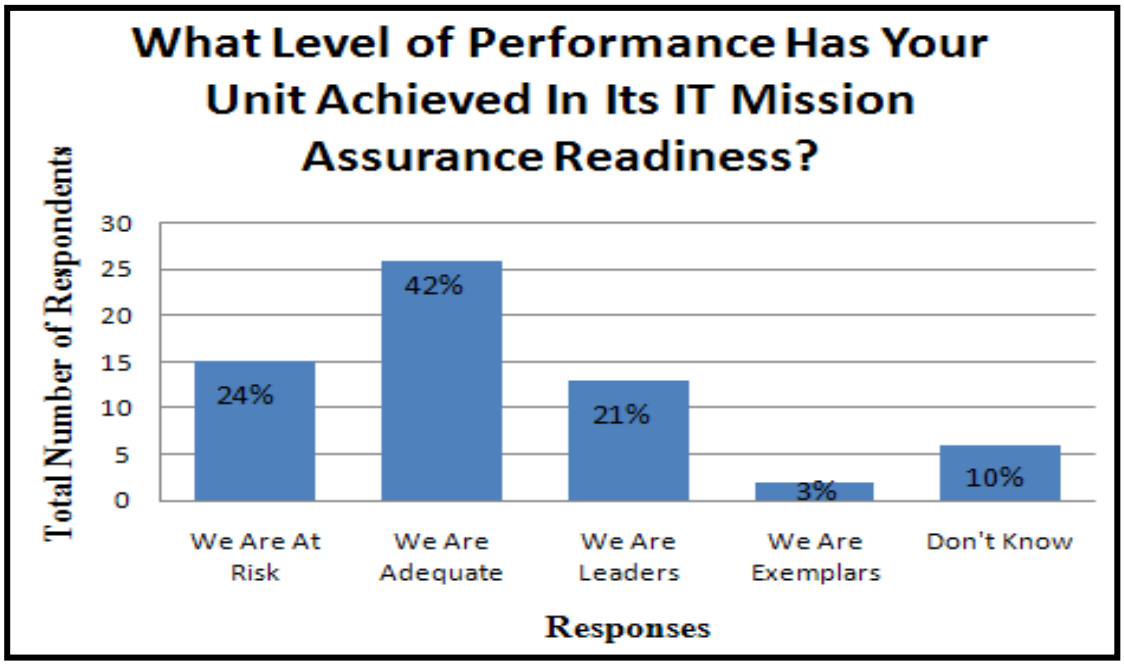

Figure 18: Self-Assessment of Level of Performance Achieved

IV. Challenges and Survey Analysis

Challenges

Throughout this paper several challenges to cyber mission assurance were explicitly identified. These challenges include:

- Develop a common lexicon for mission assurance linked to the strategic, operational, and tactical levels
- Cyber mission assurance is cross functional. One has to look beyond the communications unit
- Develop tools that can map network topology to mission requirements and mission impact
- Mission Assurance planning, to be effective, must be documented, tested
- Current OSD efforts do not help mission assurance within the boundaries of an installation
- DIACAP is not effective
- Leadership is lacking

What follows is a discussion of each of the challenges.

Develop a common lexicon for mission assurance linked to the strategic, operational, and tactical levels.

Developing a common language is an absolutely critical step towards mission assurance. Not only is it important within the cyber community but it's equally as important to the operational communities. Likewise, due to those characteristics of networks that make it difficult to identify where one ends and another begins and the difficulty in linking network assets to specific packets of data supporting any given mission, a common language will help with coordination efforts among the services, civilian enterprises and the military's of other countries.

Linking the language to the three levels of war, where possible, will also assist in the development of doctrine and policies that will further the effort to accomplish true

mission assurance. Going even further, DoD should establish academic options for military planners, like is similarly done for other niche specialties.

Cyber mission assurance is cross functional. One has to look beyond the communications unit.

Limiting the responsibility for cyber mission assurance to the communications/cyber community is absolutely the wrong thing to do. True mission assurance efforts cross functional boundaries, requires a holistic view of the objective (cyber, operations, logistics, etc.), and takes time and forethought. While it is true that each of the functional communities need to look at their internal processes to develop redundancies and back-ups, the real power of mission assurance comes when those same communities come together to synergistically provide solutions.

The other aspect of cross functionality involves the benefits of coordination and deconfliction. Just as a JFACC deconflicts aircraft entering the airspace identified in an ATO, cyberspace should be deconflicted for the same purposes. For example, if cyber assets or data are going to be brought to bear or used during a mission, someone should be ensuring that the assets or data needed for the mission are received in a timely fashion. Someone should be making sure that preventative maintenance is not scheduled for a cyber asset during a critical time. Someone should be ensuring that large amount of data are not going through a critical node, effectively slowing down the receipt of the mission essential data. Deconfliction and coordination among functional communities can provide this function but it needs to be explicitly planned for. The challenge is defining the role of and determining who the Joint Forces Cyber Component Commander (cyber JFACC equivalent) is. In a traditional air campaign, the JFACC is usually determined by

the service with the preponderance of air assets in the AOR. In the cyber world, how do you determine who has the preponderance of cyber assets? The difficulty in answering that question may mean that determining who the JFCCC is, may have to be determined another way.

Develop tools that can map network topology to mission requirements and mission impact.

There is a severe shortage in the tools available to assist with accomplishing mission assurance and cyber mission assurance. There are many tools available that can map networks and alert administrators to conditions that cause an alarm. However, what is lacking from these tools is the ability to link specific assets to specific missions. This is by no means an easy task but one that is essential. The complexity is multi-dimensional; IP routing characteristics, operational mission requirements and planning, changing networks, and Internet dynamics are but a few of the considerations.

Just as there is a requirement to link network topology to mission requirements, there also exists the need for tools to assist in understanding the impact to mission in the event of a cyber incident. Some research is underway [37] [38], but more needs to be done.

Mission Assurance planning, to be effective, must be document and tested.

An undocumented plan is merely hyperbole and a documented plan that has not been thoroughly tested is hope in written form. This is especially true in the military environment where PCSs and TDYs are a normal part of the routine of daily life. Every plan must be written, and tested periodically. There also needs to be a routine put in place to review every plan and update it accordingly. Missions, organizations, and

especially networks, change routinely and accommodations to those changes should be instituted.

Even where there are requirements for written and tested plans, as in the case with DIACAP, as previously mentioned, units often fail miserably when following through with the requirements. To solve this problem, system owners need to be held accountable for their failure to meet standards. The 'Air Force' cannot speak of the importance of ensuring mission success yet look the other way when systems fail to meet standards. It is simply unacceptable and until they're held accountable, nothing will change.

Current OSD efforts do not help mission assurance within the boundaries of an installation.

The DoD has put into place what appears to be a serious effort, to correctly address cyber mission assurance. There are some obvious areas for adjustments and improvements as has previously been discussed. The department should exercise caution in succumbing to the belief that they have addressed the entire issue.

DoDs GIG mission assurance effort does nothing to address the mission assurance efforts within the perimeter of an installation's fence. Nor does it address systems and capabilities beyond those provided by the GIG. One cannot argue the importance of assuring the capabilities of the GIG, but it is a fallacy to believe that DoD's responsibility ends there.

The department should investigate ways in which a tiered approach can be designed and implemented that would force mission assurance activities down through every level until it reaches the very fundamental levels of war fighting. Once in place the

adherence to the standard should be reported and those found lacking should be held accountable.

DIACAP is not effective.

The DIACAP process is overwhelming not effective. It is evident in its cumbersome implementation and in the IG report detailing across the board non-compliance. What is perhaps worse is that DIACAP provides a misleading sense that, at least for mission critical systems, things are being done the right way. Leaders who believe that all is well, just because a system exists that requires a mission assurance plan, would be sadly mistaken.

In May 2009, the Eighth Report Card on Computer Security at Federal Departments and Agencies was presented to Congress [39]. The report documents compliance with FISMA. The overall government wide grade was a C. For the Department of Defense, the grade was a D-, up from an F the previous year. Clearly DIACAP, the process of choice for FISMA compliance, is broken.

Leadership is Lacking.

The failure of leadership to act on the importance of mission assurance planning is arguably the single most important challenge. Leadership recognition of the problem is not enough. Accountability, funding, and attention to the issue are required. History has shown that it sometimes takes a significant adverse event to motivate action. It seems as if that may be the course for cyber mission assurance.

In his testimony to the Senate Select Committee on Intelligence concerning the annual threat assessment of the intelligence community on 12 February 2009, Dennis Blair, U.S. Director of National Intelligence spoke of the growing cyber and organized

crime threat to the United States [40]. Additionally, the survey presented in this paper showed the historical record for incidents that impaired day-to-day operations at base units. The risk to mission assurance is real and leadership has to take a more active role.

Survey Analysis

Several pertinent points can be drawn from the data presented from the mission assurance survey conducted as a part of this research. The points include:

- Disparity between guard/reserve and active duty units
- Inadequate documentation and testing
- Most disruption are caused by supporting infrastructure
- Units need funding and guidance
- IT is critical to bases mission
- Technology, funding, and leadership are primary barrier to mission assurance

What follows is a discussion of each of the points.

Disparity between guard/reserve and active duty units.

One interesting point is that there seems to be a disparity in the way in which active duty and guard/reserve units engage in mission assurance activities. In almost every case, the positive indicators were higher for guard/reserve units than for their active duty counterparts. This could be due to several factors. One is that due to the part-time nature of the guard/reserve units, the requirement for written plans may be more significant than for the active duty units. Another is that, as was noted previously, the civilian sector has done more with mission assurance and guard/reserve Airmen may be bringing that experience with them into their military service.

Inadequate documentation and testing.

By and large, units are not documenting mission assurance efforts and are not testing the plans, where they do exist, in a realistic environment. Where plans do exist,

they also seem to be shelved; having met the initial requirement to create one, their value is now obsolete.

Most disruptions are caused by supporting infrastructure.

Despite all the discussion about the threat of cyber attacks and malware, the survey shows the primary disruptions are caused by mechanical issues such as HVAC and electricity. This would suggest that elements fundamental to any network operations facility have not been provided the attention they need in order to ensure network assets are readily available. If there were a Maslow's hierarchy of needs for mission assurance, surely basic electrical and HVAC infrastructure would be lower on the scale then linking network components to operational missions. Take care of the easy stuff first.

Units need funding and guidance.

Adding to the difficulty at base level is a lack of funding and guidance from higher echelons. Units are interested in performing better at mission assurance but they lack the resources and guidance to carry it out. Unfortunately, this is a pervasive problem affecting all aspects of the military and one which will be difficult to overcome.

IT is critical to a base's mission.

This seems obvious but worth stating. IT touches every single aspect of how the military operates. From filling out a travel voucher in the Defense Travel System, to moving an ATO electronically to the AOC, to defending the network against cyber attack, IT is crucial. The value of this information is that it can and should be used to persuade those who need IT (basically everyone) to invest in its availability.

Technology, funding, and leadership are primary barriers to mission assurance.

It's interesting that technology limitations were identified as the number one barrier to mission assurance. This speaks to the previous discussion on the need for tools that automate the effort. However, in light of the previous observation that the primary cause of disruptions are mechanical issues, perhaps the respondents were identifying the need for upgrades to supporting infrastructure. Regardless, additional funding and research will go a long way to fix this problem.

V. Conclusion and Future Research

Two quotes from current leaders in the cyberspace arena illustrate the importance of mission assurance. At the 26th National Space Symposium held in Colorado Springs, Colorado in April 2010, General C. Robert Kehler, Air Force Space Command Commander outlined three objectives for cyberspace. One of those objectives he identified as, "Focusing on mission assurance rather than attempting to defend the entire network [41]." 24th Air Force Commander, Maj. Gen. Richard E. Webber stated on 25 January 2010, during the Initial Operational Capabilities announcement for 24th AF that "Cyber mission assurance is a top priority of the Air Force. The domain we are tasked to operate within touches every part of the Air Force and joint mission [42]."

This research investigated current cyber mission assurance efforts and guidance available in both the public and private sector. The literature shows a lack of guidance and accountability, particularly in the Department of Defense. It also reflects an increased importance applied to mission assurance, but efforts have not caught up with intentions. There also exist many opportunities for academic institutions and research facilities to help by developing network mapping tools, standardizing terms, and developing reporting systems that depend less on human intervention.

The data from the survey indicate a desire, at base-level, for stronger leadership and better resources for conducting mission assurance efforts. It further illustrates that some very basic activities can be acted upon to increase the mission assurance capabilities at base-level such as modernizing supporting infrastructure, documenting and testing current procedures, and developing a strong and consistent message with base leadership that illustrate the importance of mission assurance planning.

It seems clear that mission assurance, and in particular cyber mission assurance, is important to the Air Force's senior leaders. It is also equally as clear that there remains a lot to be done to be effective at accomplishing it. Changing the paradigms that exist will not be easy and it will take the collective efforts of senior leaders, industry partners, academic institutions, and operators to develop solutions.

Future Research

Much remains to be done to solve cyber mission assurance problems. As such, what follows are proposed areas for future research.

Develop roles and responsibilities for cyber mission assurance at the strategic, operational, and tactical levels of war.

Linking the importance of cyber mission assurance to the three levels of war could help establish responsibilities at each level and develop important links between activities at each level. Mission assurance, to be effective has to be fully coordinated among entities at all levels.

Research and develop tools that can map network topology to mission requirements and mission impact.

Providing simple features such as effective redundancy are impossible without knowing what is traversing the network and how the data links to ongoing missions. Beyond redundancy, knowledge of device-to-mission relationships is integral to achieving cyber mission assurance.

Analysis and research of possible mission assurance reporting structures.

A defined process for reporting the status of mission assurance is required. Risks for devices and missions at one level may affect those at another and a reporting structure that allows various entities to view the status up and down the chain of command is

essential. Ideally, the structure would support the inheritance of risk where appropriate. A Status of Resources and Training System (SORTS) like reporting structure should be examined

Research link between cyber mission assurance, risk management, and situational awareness.

These three activities share common traits such as device level status requirements, mapping of device-to-mission and mapping of device-to-risk. Identifying the common traits and how they are applied to each activity could impact the way in which future solutions are derived.

Develop methodologies and templates to standardize cyber mission assurance processes at base level.

Each base is reinventing the way in which cyber mission assurance is conducted at base level, wasting manhours. Developing a template will enhance effectiveness, standardize procedures, and improve outcomes. Standardizing processes have the added benefit of being inspectable, therefore increasing accountability.

Analysis of DIACAP and development of proposed solution to resolve the mission assurance compliance aspect that is broken.

DIACAP is broken with regards to mission assurance and continuity of operations. There may be value added in research that investigates where and why it's broken and suggesting fix actions.

Research DoD GIG cyber mission assurance efforts and propose extensions of that effort onto installations.

Capitalizing on the current GIG effort to extend it beyond the point-of-presence on a base is an area worth further research. Mission assurance requires a holistic approach and joining base-level efforts with GIG efforts makes sense.

Examine and propose the role of a Joint Forces Cyber Component Commander.

Someone has to control the cyberspace domain to support missions just as a JFACC controls airspace in an AOR. The Joint Forces Cyber Component Commander could fulfill such a role but traditional methods to identify a JFACC (ownership of the preponderance of air assets) won't work in identifying a JFCCC. Research into what role a JFCCC would play and how to identify who fills that role could prove beneficial.

Appendix A. Survey Questions

Survey Overview

Thank you for taking part in this study being conducted by a graduate student at the Air Force Institute of Technology. The goal of the project is to determine mission assurance planning efforts at base-level communications squadrons and the factors affecting those efforts. More specifically, this survey focuses on mission assurance planning efforts affecting computer network operations that provide core IT services for the base.

Mission assurance planning, for the purposes of this survey, are those efforts to establish contingency plans to mitigate, recover from, and reestablish network operations if an event occurs that reduces normal day-to-day operations. Again, for the purposes of this survey, mission assurance planning is synonymous with 'continuity of operations planning (COOP)', 'contingency operations planning', and 'crisis planning.'

About You

1. Your position
    a. Commander
    b. Deputy Commander/Director of Operations
    c. Operations Flight Commander
    d. Plans and Programs Flight Commander
    e. Action Officer
    f. Other

2. I am personally very involved in IT mission assurance in my unit.
    a. Strongly disagree
    b. Disagree
    c. Neutral
    d. Agree
    e. Strongly agree

3. How long have you been in the unit?
    a. Less than 1 year
    b. 1 year
    c. 2 years
    d. 3 years
    e. 4 year
    f. 5 years
    g. More than 5 years

Base Plan

4. Does your installation have a formal, documented plan for overall mission assurance?
    a. No plan currently in place <Go to question 9>
    b. Plan is being developed
    c. Plan is complete, but needs updating
    d. Plan is complete and up to date

5. When was the last time the installation's mission assurance plan was exercised?
    a. Last 6 months
    b. 6 months to 1 year
    c. 1 to 2 years
    d. 2 + years
    e. I don't know <Go to Question 7>

6. To what extent was the installation's mission assurance plan exercised?
    a. Table top exercise
    b. Scheduled test (could include ORI)
    c. Complete unannounced test
    d. Other

7. Does your installation have an appointed individual responsible for mission assurance planning?
    a. Yes
    b. No
    c. I don't know

8. Is IT a specific part of the installation's plan?
    a. Yes
    b. No

NOSC Plan

9. Do you receive any IT services from a higher level NOSC?
    a. Yes
    b. No <Go to question 15>

10. Does the NOSC have a formal, documented plan for IT mission assurance?
    a. No plan currently in place <Go to question 15>
    b. Plan is being developed
    c. Plan is complete, but needs updating
    d. Plan is complete and up to date

11. When was the last time the NOSC's mission assurance plan was exercised?
    a. Last 6 months
    b. 6 months to 1 year
    c. 1 to 2 years
    d. 2 + years
    e. I don't know <Go to Question 15>

12. To what extent was the NOSC's mission assurance plan exercised?
    a. Table top exercise
    b. Scheduled test (could include ORI)
    c. Complete unannounced test
    d. Other

13. Is there a specific NOSC POC for mission assurance planning?
    a. Yes
    b. No
    c. I don't know

14. Are the services you receive from the NOSC covered in the NOSC mission assurance plan?
    a. Yes
    b. No

Unit Plan

15. Does your unit have a formal, documented IT mission assurance plan?
    a. No plan currently in place <Go to question 23>
    b. Plan is being developed
    c. Plan is complete, but needs updating
    d. Plan is complete and up to date

16. When was the last time your unit's mission assurance plan was exercised?
    a. Last 6 months
    b. 6 months to 1 year
    c. 1 to 2 years
    d. 2 + years
    e. I don't know <Go to Question 18>

17. To what extent was the unit's mission assurance plan exercised?
    a. Table top exercise
    b. Scheduled test (could include ORI)
    c. Complete unannounced test
    d. Other

18. Is there a specific unit POC for mission assurance planning?
    a. Yes
    b. No
    c. I don't know

19. What is the number ONE driver for IT mission assurance planning at your base?
    a. Threat of Cyber Attack
    b. Threat of Virus/malware execution
    c. Terrorism
    d. Criticality of IT resources to mission
    e. Geographic threats (earthquake zone, flooding area, etc.)
    f. Wing/MAJCOM requirement
    g. NOSC requirement
    h. Severe weather (hurricane, storm, etc.)
    i. Other

20. What is the number TWO driver for IT mission assurance planning at your base?
    a. Threat of Cyber Attack
    b. Threat of Virus/malware execution
    c. Terrorism
    d. Criticality of IT resources to mission
    e. Geographic threats (earthquake zone, flooding area, etc.)
    f. Wing/MAJCOM requirement
    g. NOSC requirement
    h. Severe weather (hurricane, storm, etc)
    i. Other

21. What are the primary barriers to IT mission assurance planning at your base? Select up to two.
    a. Funding
    b. Manpower constraints
    c. Technology limitations
    d. Lack of leadership support
    e. Difficulty in customer's ability to define mission critical data/processes
    f. Other

22. Has your unit been contacted in support of other units' mission assurance efforts?
    a. Yes
    b. No
    c. I don't know

Potential Conflicts

23. Does the NOSC and your base have a mission assurance plan that includes your unit?
    a. Yes
    b. No <Go to question 26>
    c. I don't know <Go to question 26>

24. Are there conflicts for the unit between the two plans?
    a. Yes
    b. No <Go to question 26>
    c. I don't know <Go to question 26>

25. Rate the severity of the conflict based on its impact to the unit
    a. Minimal impact to the unit
    b. Marginal impact to the unit
    c. Serious impact to the unit

Mission Assurance Funding

26. Does your unit receive funding specifically for mission assurance planning and/or implementation of mission assurance measures?
    a. Yes
    b. No <Go to question 29>
    c. I don't know <Go to question 29>

27. Where does funding come from for mission assurance planning and/or implementation (select all that apply)?
    a. Base
    b. NOSC
    c. MAJCOM
    d. Unit budget
    e. Unfunded requirement
    f. Other

28. In this fiscal year's budget, on what are you spending your mission assurance funds?
    a. Contractor expertise
    b. Training
    c. Hardware
    d. Software
    e. HVAC upgrades
    f. Electrical upgrades
    g. Offsite facilities
    h. Other

Incident History

29. In the past 5 years, has your unit experienced any disruptions to normal IT operations that caused you to implement formal or ad hoc emergency response procedures?
    a. Yes
    b. No <Go to question 37>
    c. I don't know <Go to question 37>

30. How many disruptions have occurred in the last 5 years?
    a. 1
    b. 4
    c. 7
    d. 2
    e. 5
    f. 8
    g. 3
    h. 6
    i. 9

31. Concerning the two most significant disruptions, select the triggering event(s)

    a. Electrical failure
    b. Cable cut
    c. Cyber attack
    d. Virus/malware outbreak
    e. Flood
    f. Fire
    g. Hardware failure
    h. Software failure
    i. HVAC failure
    j. Tornado
    k. Earthquake
    l. Other severe weather
    m. Other

32. Based on the triggering events in question 28, has your installation experienced any of the following consequences from the disruptions? Select all that apply

    a. Network unavailable
    b. Web site unavailable
    c. E-mail unavailable
    d. Application(s) unavailable
    e. Damage to hardware
    f. Damage to software
    g. Damage to data
    h. Other

33. Briefly describe the disruption that had the most impact.

34. Briefly describe your response to the disruption described above.

35. Rate the size of the impact of this specific disruption:
    a. No effect on facilities/processes
    b. Affected a few facilities/processes
    c. Affected many facilities/processes
    d. Affected the entire base

36. Rate the mission impact of this specific disruption.
    a. No impact to the mission
    b. Little base-wide mission impact
    c. Moderate base-wide mission impact
    d. Significant base-wide mission impact

Final Assessment

37. If IT services and electronic data were unavailable, other units on base would be able to carry out their mission critical tasks.
    a. Strongly disagree
    b. Disagree
    c. Neutral
    d. Agree
    e. Strongly agree

38. My unit is prepared to restore mission critical systems in the event of a disruption
    a. Strongly disagree
    b. Disagree
    c. Neutral
    d. Agree
    e. Strongly agree

39. My unit is better prepared to restore mission critical systems today than it was 2 years ago.
    a. Strongly disagree
    b. Disagree
    c. Neutral
    d. Agree
    e. Strongly agree

40. What level of performance has your unit achieved in its IT mission assurance readiness?
    a. We are at risk
    b. We are adequate
    c. We are leaders
    d. We are exemplars
    e. Don't know

41. What type of unit are you reporting on?
    a. Active duty
    b. Guard
    c. Reserves

Bibliography

1. **DoD Inspector General.** Contingency Planning for DoD Mission-Critical Information Systems. Washington DC : s.n., 2008. Report No. D-2008-047.

2. **William J. Lynn III, Deputy Secretary of Defense.** DoD Policy and Responsibilities for Critical Infrastructure. *DoD Directive.* s.l. : Department of Defense, January 14, 2010. Number 3020.40.

3. *Mission Impact: Role of Protection of Information Systems.* **Anderson, E., Choobineh, J. Fazen, M., and Grimaila, M.R.** Wright-Patterson AFB, OH : Academic Publishing Limited, 2010. 5th International Conference on Information Warfare and Security.

4. *Mission Impact of Cyber Events: Scenarios and Ontology to Express the Relatioinships Between Cyber Assets, Missions and Users.* **Anita D'Amico, Laurin Buchanan, John Goodall, and Paul Walczak.** Wright-Patterson AFB, OH : Academic Publishing Limited, 2010. 5th International Conference on Information Warfare and Security.

5. *Communicating Potential Mission Impact Using Shared Mission Representations.* **Hale, B. Grimaila, M.R., Mills, R.F., Haas, M., and Maynard, P.** Wright-Patterson AFB, OH : Academic Publishing Limited, 2010. 5th International Conference on Information Warfare and Security.

6. *AIMFIRST: Planning for Mission Assurance.* **Haigh, T., Harp, S., and Payne, C.** Wright-Patterson AFB, OH : Academic Publishing Limited, 2010. 5th International Conference on Information Warfare and Security.

7. *Evaluating the Impact of Cyber Attacks on Missions.* **Musman, S., Temin, A., Tanner, M., Fox, D., and Pridemore, B.** Wright-Patterson AFB, OH : Academic Publishing Limited, 2010. 5th International Conference on Information Warfare and Security.

8. **Committee of Sponsoring Organizations.** About Us. *Committee of Sponsoring Organizations of the Treadway Commission.* [Online] [Cited: March 9, 2010.] http://www.coso.org/aboutus.htm.

9. *Tone at the Top.* Altamonte Springs, FL : THE INSTITUTE OF INTERNAL AUDITORS, 2005. Issue 28.

10. **U.S. Congress.** Sarbanes-Oxley Act of 2002. 2002. Public Law 107-204.

11. **Steele, John.** Enterprise-Wide Risk Management - Top 10 Things Everyone should know about Enterprise Risk Management. *Information Systems Audit and Control Association - Victoria Chapter.* [Online] February 2006. [Cited: March 18, 2010.] http://www.isacavictoria.ca/presentations/Feb%2006%20Steele%20Enterprise%20risk%20management.ppt.

12. *Enterprise Risk Management - Integrated Framework.* **Committee of Sponsoring Organizations of the Treadway Commission, John J. Flaherty Chairman.** September 2004, p. 2.

13. **Walters, Jonathan.** *Transforming Information Technology at the Department of Veterans Affairs.* The IBM Center for The Business of Government. 2009.

14. IT Governance Case Study US House of Representatives Implements IT Governance. *IT Governance Institute.* [Online] July 2002. [Cited: March 17, 2010.] http://www.itgi.org/Template_ITGI.cfm?Section=Case_Studies1&CONTENTID=9193&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

15. COBIT and IT Governance Case Study: Sun Microsystems. *IT Governance Institute.* [Online] June 2005. [Cited: March 18, 2010.] http://www.itgi.org/Template_ITGI.cfm?Section=Case_Studies1&CONTENTID=50160&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

16. *CoBiT 4.1 Excerpt, Executive Summary.* ROLLING MEADOWS, IL : IT Governance Institute, 2007.

17. In A Nutshell: A Short History of ITIL. *ITIL Central.* [Online] 2005. [Cited: April 24, 2010.] http://itsm.fwtk.org/History.htm.

18. **UK Office of Government Commerce.** About ITIL. *Official ITIL® Website.* [Online] April 8, 2010. [Cited: April 24, 2010.] http://www.itil-officialsite.com/AboutITIL/WhatisITIL.asp.

19. IT Service Continuity Management. *ITIL Library Open Guide.* [Online] [Cited: April 24, 2010.] http://www.itlibrary.org/index.php?page=IT_Service_Continuity_Management.

20. **UK Office of Government Commerce.** *Service Delivery Book.* London, UK : The Stationery Office, 2001. 9780113300174 .

21. About ISO. *www.iso.org.* [Online] 2010. [Cited: March 31, 2010.] http://www.iso.org/iso/about.htm.

22. ISO publishes international benchmark for incident preparedness and operational continuity management . *International Standards Organization.* [Online] November 29, 2007. [Cited: AprIL 25, 2010.] http://www.iso.org/iso/pressrelease?refid=Ref1094.

23. **Published as a news service by IHS.** ISO Publishes Benchmark for Incident Preparedness, Operational Continuity Management - ISO PAS 22399. *IHS.* [Online] December 5, 2007. [Cited: April 24, 2010.] http://aero-defense.ihs.com/news/iso-incident-preparedness.htm.

24. **U.S. Congress.** The Computer Security Act of 1987 . Public Law No: 100-235.

25. **United States Congress.** Paperwork Reduction Act of 1995. Washington DC : s.n., January 4, 1995.

26. **U.S. Congress.** Clinger Cohen Act of 1996. Public Law 104-106, Division E.

27. **U.S. Congress.** Federal Information Security Management Act. *Title III of the E-Government Act of 2002* . Public Law 107-347.

28. **Office of Management and Budget.** CIRCULAR NO. A-130. *Whitehouse.gov.* [Online] [Cited: April 24, 2010.] http://www.whitehouse.gov/omb/circulars_a130_a130trans4/.

29. Public and Business Affairs. *National Institutes of Standards and Technology.* [Online] April 3, 2010. [Cited: April 25, 2010.] http://www.nist.gov/public_affairs/general_information.cfm.

30. Federal Information Processing Standards Publications. *Information Technology Laboratory.* [Online] September 2, 2008. [Cited: April 25, 2010.] http://www.itl.nist.gov/fipspubs/geninfo.htm.

31. **ASD(NII)/DoD CIO.** DoD Information Assurance Certification and Accreditation Process. Washington DC : Department of Defense, 2007. NUMBER 8510.01.

32. Network Resilience & Cyber Mission Assurance. *Intelink* . [Online] October 9, 2009. [Cited: March 15, 2010.] https://www.intelink.gov/wiki/Network_Resilience_%26_Cyber_Mission_Assurance.

33. Statement by Mr Robert F. Lentz, Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance before the U.S. House of Representatives Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities. Washington DC : s.n., 2009.

34. **Lt Gen Ronald F. Sims.** *Inspector General Activities.* Washington DC : Secretary of the Air Force, 2009. AFI 90-201.

35. **Christopher J. Alberts, Audrey J. Dorofee.** *Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments.* Pittsburgh, PA : Carnegie Mellon University, 2005.

36. NETWORK OPERATIONS (NETOPS). Washington DC : U.S. Air Force, 2006. AFI 33-115V1.

37. *An Automated Information Asset Tracking Methodology to Enable Timely Cyber Incident Mission Impact Assessment.* **M.R. Grimaila, R.F. Mills, L.W. Forston.** Bellevue, WA : Proceedings of the 2008 International Command and Control Research and Technology Symposium, 2008.

38. *An Architecture for Cyber Incident Mission Impact Assessment.* **D. Sorrels, M. R. Grimaila, L. W. Forston, R. F. Mills.** Omaha, NE : Proceedings of the 2008 International Conference on Information Warfare and Security, 2008.

39. **Davis, Tom.** *Eighth Report Card on Computer Security at Federal Departments and Agencies.* Washington DC : House Oversight and Government Reform Committee, 2008.

40. **Blair, Dennis.** *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* . 2009. SSCI ATA Feb 2009 - IC Statement for the Record.

41. Cyber 1.0 Event. *26th National Space Symposium.* [Online] April 12, 2010. [Cited: April 24, 2010.] http://2010.nationalspacesymposium.org/media/news-briefs/kehler-and-pulham-kick-off-cyber-10.

42. Air Force Cyber Numbered Air Force Achieves Initial Operational Capability. *The Official Web Site for the U. S. Air Force.* [Online] January 25, 2010. [Cited: May 6, 2010.] http://www.af.mil/news/story.asp?id=123187145.

Vita

Major Mickey R. Evans graduated from Crisfield High School in Crisfield, Maryland. He enlisted in the U.S. Air Force in January 1988 and went on to serve more than seven years on active duty as an enlisted airman. He received his undergraduate degree from the University of Southern Mississippi in Computer Science and was commissioned through the Reserve Officer Training Program in August 1997. He received his graduate degree from Webster University in June 2000 in Computer Resources and Information Management.

His first assignment in October 1997, was at HQ Air Mobility Command, Scott AFB, Illinois, as a computer systems program manager. In July 2000, he was assigned to the 72nd Test and Evaluation Squadron at Whiteman AFB, Missouri where he served as a flight commander for B-2 Data Services. He then was assigned to the Defense Intelligence Agency, Bolling AFB, Washington DC in July 2003 where he served as an information technology program manager and branch chief. In June 2006, he was assigned to the 1st Communications Squadron, Langley AFB, Virginia where he served as both a flight commander and the deputy squadron commander. While stationed at Langley he deployed to Iraq and Germany.

In 2009 he entered the Cyber Warfare program, Graduate School of Engineering and Management, Air Force Institute of Technology. Upon graduation, he will take command of Detachment 2, 561 Network Operations Squadron at Randolph AFB, TX.

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to an penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**			
1. REPORT DATE *(DD-MM-YYYY)* 03-06-10	**2. REPORT TYPE** Graduate Research Project		**3. DATES COVERED** *(From – To)* Jun 2009 – Jun 2010
4. TITLE AND SUBTITLE An Informational Analysis and Communications Squadron Survey of Cyberspace Mission Assurance			**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Maj Mickey R. Evans			**5d. PROJECT NUMBER** N/A **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Dr. Doug Kelly, Cyber Team Lead 711th Human Performance Wing Air Force Research Laboratory, Human Performance Wing, Sense-making & Organizational Effectiveness Branch Building 190 WPAFB OH 45433 Comm: (937) 656-4391			**10. SPONSOR/MONITOR'S ACRONYM(S)** AFRL/HPW/RHXS **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for Public Release; Distribution is Unlimited			
13. SUPPLEMENTARY NOTES This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.			
14. ABSTRACT Networks under the Air Force's purview are under constant attack from hostile actors. The dependence on these systems by every facet of the Air Force enterprise is more prevalent now than ever before. The realization of these facts has increased the focus on assuring more than the network systems and applications themselves, but instead on the missions that rely so heavily on the systems. The purpose of this research was to investigate the current state of cyber mission assurance efforts and guidance available in both the public and private sector and to establish the realities facing base level units. Specifically, this graduate research project sought to answer two research questions addressing guidance and unit realities: What, if any, regulatory guidance is available, to include processes, procedures, and directives, both public and private? To what extent do base-level units perform cyber mission assurance activities and what factors influence their efforts? The research questions were answered through a comprehensive literature review, and the development and use of a survey. The research identified the presence of minimal regulatory requirements and a need for consistent guidance, policy and procedures. It also identified trends at units with the task of providing services. The culmination of this effort was the identification of several challenges facing researchers and data from base-level units relevant to the discussion.			
15. SUBJECT TERMS Mission Assurance; Cyberspace Mission Assurance;			
16. SECURITY CLASSIFICATION OF:	**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Michael R. Grimaila (ENV)
REPORT U / **ABSTRACT** U / **c. THIS PAGE** U	UU	80	**19b. TELEPHONE NUMBER** *(Include area code)* 937-255-6565, x4800 michael.grimaila@afit.edu

Standard Form 298 (Rev: 8-98)
Prescribed by ANSI Std. Z39-18